CONSULENZE PACI PRIVACY

Relatore: Dott. Antonio Carmine Didona

Contatti:
segreteria@consulenzepaci.it
Tel. Back office 0541.1798438
Tel. Segreteria 0541.1795431
www.consulenzepaci.it

CYBERSECURITY

Il presente materiale didattico è riservato e destinato alla sola formazione interna dei dipendenti, non è cedibile a terzi.

ENISA
EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY

ORGANISMO

L'ENISA, **Agenzia dell'Unione Europea per la Cybersicurezza**, è un centro di competenze in materia di sicurezza informatica in Europa. Aiuta l'UE e i paesi membri dell'UE a essere meglio attrezzati e preparati a prevenire, rilevare e reagire ai problemi di sicurezza dell'informazione.

ENISA
EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY

MALWARE

Il malware è un tipo comune di attacco informatico sotto forma di software malevolo. Le famiglie di malware comprendono cryptominer, virus, ransomware, worm e spyware. **Gli obiettivi tipici sono il furto di informazioni o di identità, lo spionaggio e l'interruzione dei servizi**.

I **protocolli web** e di **posta elettronica** sono stati i vettori di attacco iniziali più comunemente utilizzati per diffondere il malware.

ENISA
EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY

PHISHING

Il phishing è il tentativo fraudolento di rubare i dati degli utenti, come credenziali di accesso, dati della carta di credito o anche denaro, mediante tecniche di ingegneria sociale.

Questo tipo di attacco viene in genere lanciato attraverso messaggi di posta elettronica che sembrano inviati da una fonte attendibile, con l'intento di convincere l'utente ad aprire un allegato malevolo o a seguire un URL fraudolento.

ENISA
EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY

SPAM

Lo spam consiste nell'invio di messaggi non richiesti in massa. Costituisce una minaccia per la cybersicurezza quando viene utilizzato come vettore di attacco per distribuire o attivare altre minacce.

Lo spam può talvolta essere confuso o erroneamente classificato come campagna di phishing.

La differenza principale tra i due è il fatto che il **phishing** è un'azione mirata, che ha come **obiettivo il furto dei dati degli utenti**. Lo **spam** è invece una tattica per **inviare e-mail non richieste** in massa a un elenco di destinatari.

ENISA
EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY

VIOLAZIONE DEI DATI

Una violazione dei dati è un tipo di **incidente di cybersicurezza caratterizzato dall'accesso a informazioni senza la giusta autorizzazione**, in genere con intento doloso, che ha come conseguenza la potenziale perdita o il potenziale uso improprio di tali informazioni.

Secondo le ricerche dell'ENISA, **occorrono circa 206 giorni per identificare una violazione dei dati** in un'organizzazione. Pertanto, il tempo necessario per contenere, riparare e recuperare i dati significa tempi più lunghi per il ritorno alla normalità.

PRINCIPIO DI MINIMIZZAZIONE COME MISURA DI SICUREZZA

ENISA
EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY

MINACCIA INTERNA

Una minaccia interna **è un'azione che può portare a un incidente, compiuta da una persona o da un gruppo di persone affiliate alla potenziale vittima** o che lavorano per la medesima.

I **cinque tipi di minaccia interna** possono essere definiti secondo le motivazioni e gli obiettivi:

1. **lavoratori negligenti** che trattano impropriamente i dati, violano le politiche di utilizzo e installano applicazioni non autorizzate;
2. agenti interni che rubano informazioni **per conto di terzi**;
3. **dipendenti insoddisfatti** che cercano di danneggiare la loro organizzazione;
4. **insider malintenzionati** che sfruttano i privilegi esistenti per rubare informazioni a scopo di guadagno personale;
5. **terzi irresponsabili** che compromettono la sicurezza attraverso l'intelligence, l'uso improprio o l'accesso a un asset o il suo utilizzo per finalità malevole.

ENISA
EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY

RANSOMWARE

Il ransomware **è un programma informatico dannoso che può infettare un dispositivo digitale, bloccando l'accesso a tutti o ad alcuni dei suoi contenuti per poi chiedere un riscatto da pagare per liberarli**.

Esistono due tipi principali di ransomware:

1. **i cryptor** → criptano i file contenuti nel dispositivo rendendoli inaccessibili;
2. **i blocker** → bloccano l'accesso al dispositivo infettato.

Questo tipo di software malevoli si diffonde soprattutto attraverso **comunicazioni ricevute via e-mail, sms o sistemi di messaggistica.**

ENISA
EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY

COME DIFENDERSI

La prima e più importante forma di difesa è la prudenza. Occorre evitare di aprire messaggi provenienti da soggetti sconosciuti o con i quali non si hanno rapporti e, in ogni caso, se si hanno dubbi, non si deve cliccare su link o banner sospetti e non si devono aprire allegati di cui si ignora il contenuto.

CONSULENZE PACI PRIVACY

Relatore: Dott. Antonio Carmine Didona

GRAZIE PER L'ATTENZIONE

Contatti:
segreteria@consulenzepaci.it
Tel. Back office 0541.1798438
Tel. Segreteria 0541.1795431
www.consulenzepaci.it