CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

SESSIONE FORMATIVA ON LINE CORSO DI PERFEZIONAMENTO

CYBERSECURITY: MINACCE E MISURE DI PREVENZIONE PER GLI ATTACCHI HACKER

Autore Dott.ssa Gloriamaria Paci

Studio Paci & C. Srl
Studio Consulenza Privacy Dott.ssa Gloriamaria Paci
Via Edelweiss Rodriguez Senior, 13
47924 Rimini (Rn)

Telefono: 0541 – 1795431
Telefax: 0541 - 1794118
Cellulare: 347-5244264
Mail: info@consulenzepaci.it
Sito web: www.consulenzepaci.it

Seguici sui social!
https://linktr.ee/studiopaci

Associazione Protezione Diritti e Libertà Privacy APS
Via Edelweiss Rodriguez Senior, 13
47924 Rimini (Rn)
Tel. 0541-1795431 / Fax 0541-1794118
Cell. Gloriamaria Paci 347-5244264

segreteria@associazionedirittiprivacy.it
posta@pec.associazionedirittiprivacy.it
www.associazionedirittiprivacy.it

Seguici sui social!

https://lintr.ee/apdlp

Gloriamaria Paci

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Nata a Rimini nel gennaio del 1969, dopo alcuni anni dedicati alla carta stampata, nel 1998 Gloriamaria decide di scommettere ed investire in un settore allora poco conosciuto: la normativa sulla tutela dei dati personali.

L'esperienza di giornalista pubblicista, affiancata a quella di consulente privacy nel settore pubblico e privato, sia sul territorio italiano che in paesi Extra UE (RSM), verrà impiegata per pubblicare numerosi articoli e testi di settore.

Relatrice a convegni, seminari e corsi di formazione, con l'introduzione del Regolamento Europeo 2016/679, oggi ricopre il ruolo di Responsabile per la protezione di dati personali per privati ed enti pubblici.

Presidente dell'Associazione protezione diritti e libertà privacy, porta avanti progetti ed iniziative finalizzate all'aggregazione di quanti sono interessati alla salvaguardia dei diritti e delle libertà personali nell'ambito della protezione dei dati.

Luca Di Leo

Consulenza e formazione in materia di protezione dei dati personali dal 2005

Studio Paci & C. Srl
(cda)

Associazione Protezione diritti e libertà privacy APS
(Vice presidente)

Contatti:
dileo@studiopaciecsrl.it
Cell. 3931019939
www.consulenzepaci.it
Linkedin: #luca di leo

Responsabile della Protezione dei Dati (DPO per aziende private, pubbliche, sanità)
certificazione UNI 11697:2017 (Registro Accredia)

Valutatore Privacy
certificazione UNI 11697:2017 (Registro Accredia)

Privacy Officer
Certificazione TUV Italia 2013 – certificazione competenze Federprivacy – Legge n.4/2013

Auditor GDPR
secondo lo schema di certificazione per il GDPR: ISDP@10003 (Registro AICQ SICEV)

Consulente per l'implementazione dello schema di certificazione ISDP@10003
(Ente di certificazione INVEO)

Lead Auditor ISO 27001 , aggiornamento ISO 27701

PROGRAMMA DEL CORSO

1. **ENISA - European Network And Information Security Agency**
   - Organismo;
   - Funzioni.

2. **REPORT 2022**
   - Scenario delle minacce;
   - Analisi minacce principali.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

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

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

ENISA
EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY

FUNZIONI

L'Agenzia collabora con le organizzazioni e le imprese per rafforzare la fiducia nell'economia digitale, promuovere la resilienza delle infrastrutture dell'UE e, in ultima analisi, garantire la sicurezza digitale dei cittadini dell'UE. Ciò avviene attraverso la condivisione delle conoscenze, lo sviluppo di personale e strutture e la sensibilizzazione.

ENISA
EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY

REPORT 2022

Arco temporale analizzato dal report: luglio 2021 – luglio 2022

Il 03 novembre 2022, l'ENISA ha pubblicato **l'ottava relazione annuale "*ENISA Threat Landscape*"** (ETL), identificando e valutando le principali minacce informatiche per il periodo luglio 2021 - luglio 2022.

ENISA

EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY

REPORT 2022

Sulla base dell'analisi presentata in questo rapporto, l'ENISA identifica e si concentra sui seguenti otto principali gruppi di minacce.

1. Ransomware
2. Malware
3. Social Engineering threats
4. Threats against data
5. Threats against availability: Denial of Service
6. Threats against availability: Internet threats
7. Disinformation – misinformation
8. Supply-chain attacks

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.**

CONSULENZE PACI PRIVACY

Associazione
Protezione Diritti e Libertà
Privacy APS

PHISHING = PRINCIPALE VETTORE DI ATTACCHI RANSOMWARE

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.

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.

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.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

SOCIAL ENGINEERING

Il social engineering attacks sono delle vere e proprie strategie basate su interazioni interpersonali finalizzate a carpire informazioni riservate.

Comprendono un'ampia gamma di attività che tentano di sfruttare un errore umano o un comportamento umano con l'obiettivo di ottenere l'accesso a informazioni o servizi.

Utilizza varie forme di manipolazione per indurre le vittime a commettere errori o a consegnare informazioni sensibili o segrete. Nella sicurezza informatica, l'ingegneria sociale induce gli utenti ad aprire documenti, file o e-mail, visitare siti Web o concedere a persone non autorizzate l'accesso a sistemi o servizi.

Tali tipologie di minacce fanno sempre affidamento su un elemento umano per avere successo.

SOCIAL ENGINEERING

Principali vettori

Tra i principali vettori di tale minaccia:

- Phishing
- Spear-phishing
- Smishing
- Vishing
- Whaling
- Business e-mail compromise (BEC)

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

SOCIAL ENGINEERING

Spear-phishing

Lo spear-phishing è una versione più sofisticata del phishing che prende di mira organizzazioni o individui specifici. Le email vengono predisposte su misura per ogni vittima. L'attaccante può fingersi interessato sostenitore di una causa condivisa dal bersaglio, spacciarsi per qualcuno conosciuto dalla vittima, o utilizzare altre tecniche di social engineering per ottenere la fiducia del malcapitato.

SOCIAL ENGINEERING

Smishing

Lo Smishing (o phishing tramite SMS) è una forma di truffa che utilizza messaggi di testo e sistemi di messaggistica (compresi quelli delle piattaforme social media) per appropriarsi di dati personali a fini illeciti (ad esempio, per poi sottrarre denaro da conti e carte di credito).

SOCIAL ENGINEERING

Smishing

COME FUNZIONA?

I messaggi di smishing invitano i destinatari a compiere azioni (cliccare link, ecc.) o fornire informazioni con urgenza, per non rischiare danni (es: blocco di utenze, blocco della carta di credito o del conto) o sanzioni.

I tuffatori ("smisher") inviano ad esempio messaggi per chiedere ad esempio alle vittime di:

- cliccare un link che conduce ad un form online in cui inserire dati personali, dati bancari o della carta di credito, ecc;
- scaricare un allegato che può contenere programmi malevoli capaci di prendere il controllo dello smartphone o accedere ai dati in esso contenuti;
- rispondere ai messaggi ricevuti inviando dati personali (il codice fiscale, il PIN del Bancomat o quello utilizzato per l'Internet banking, il numero della carta, il codice di sicurezza della carta, i dati dell'OTP cioè della password temporanea per eseguire operazioni sul conto bancario e sulla carta di credito, ecc.);
- chiamare un numero di telefono, dove poi un finto operatore o un sistema automatizzato chiedono di fornire informazioni di vario tipo, compresi dati bancari e/o della carta di credito.

SOCIAL ENGINEERING

Smishing

Alcuni esempi di messaggi da valutare con particolare attenzione e cautela:

- una banca o un gestore di carte di credito o una società di recupero crediti che segnalano un account compromesso, generici problemi tecnici o anomalie sul conto bancario o sulla carta di credito, da verificare urgentemente, ecc.;
- offerte di sconti straordinari su beni e servizi, o anche proposte di ricariche telefoniche da effettuare subito a costi incredibilmente vantaggiosi;
- fornitori di beni o servizi che segnalano bollette o rate non pagate da saldare con urgenza; pacchi, lettere o raccomandate da ritirare o che si ha difficoltà a consegnare, ecc.;
- amministrazioni pubbliche che segnalano la necessità di fornire dati, sanzioni da pagare (multe, cartelle esattoriali), anomalie da verificare, ecc.;
- piattaforme che offrono servizi di social media o di messagistica che segnalano una violazione dell'account personale e chiedono di fornire dati e/o compiere determinate azioni (cliccare link, compilare form, chiamare numeri o inviare messaggi, ecc.).

SOCIAL ENGINEERING

Vishing

Il vishing (o phishing vocale) è una forma di truffa, sempre più diffusa, che utilizza il telefono come strumento per appropriarsi di dati personali - specie di natura bancaria o legati alle carte di credito - e sottrarre poi somme di denaro più o meno ingenti.

Di solito le vittime vengono contattate telefonicamente da finti operatori (di banche o di società che gestiscono bancomat o carte di credito) i quali, con la scusa di presunte "anomalie", chiedono alle persone, nel loro stesso interesse, di collaborare a mettere in campo necessarie (e false) "procedure di sicurezza".

I visher fanno leva sul timore legato ad un rischio incombente per convincere le vittime ad abbassare il livello di prudenza e a reagire d'impulso. Una particolare forma di ingegneria sociale che dimostra una elevata efficacia.

SOCIAL ENGINEERING

Whaling

Il Whaling è un particolare attacco di spear-phishing rivolto a dirigenti e vertici aziendali quali CEO, CFO, CIO e in generale tutti quei profili che all'interno di un'azienda sono in possesso sia di informazioni strettamente riservate che di elevati poteri decisionali e di spesa.

L'obiettivo è quello di manipolare la vittima inducendola con l'inganno a divulgare informazioni in suo possesso o a fargli compiere specifiche azioni dannose per l'azienda ma remunerative per l'attaccante, come ad esempio autorizzare un bonifico a beneficio di quest'ultimo

SOCIAL ENGINEERING

Business e-mail compromise (BEC)

Business E-mail Compromise (BEC) è una sofisticata truffa rivolta ad aziende e organizzazioni, in cui i criminali utilizzano tecniche di ingegneria sociale per ottenere l'accesso all'account di posta elettronica di un dipendente o dirigente per avviare bonifici bancari in condizioni fraudolente.

ULTERIORI MINACCE

RILEVANTI

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

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.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

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

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.

COME AFFRONTARLE

Le raccomandazioni possono articolarsi in tre categorie:

1. Le persone

Le persone svolgono un ruolo essenziale nell'ecosistema della sicurezza informatica. Il rapporto richiama l'attenzione sull'importanza della responsabilità e della consapevolezza dei dipendenti, della formazione e delle politiche di sicurezza informatica, nonché della gestione di terze parti in relazione a informazioni riservate e/o sensibili.

COME AFFRONTARLE

Le raccomandazioni possono articolarsi in tre categorie:

2. Processi

Il monitoraggio dei processi aziendali interni include l'esecuzione di audit, pianificazione e risposta agli incidenti, password, patch software e protezione dei dati.

COME AFFRONTARLE

Le raccomandazioni possono articolarsi in tre categorie:

3. Tecnico

A livello tecnico, dovrebbero essere considerati una serie di aspetti in relazione alla sicurezza della rete, antivirus, crittografia, monitoraggio della sicurezza, sicurezza fisica e protezione dei backup.

Grazie per l'attenzione

CONSULENZE PACI PRIVACY

Associazione
Protezione Diritti e Libertà
Privacy APS