Corso di aggiornamento

Corso di formazione Cybersecurity base

Mercoledì 9 novembre 2022 in orario **9:00 – 13:00**
Webinar online

DOCENTE

Dott.ssa Giulia Gradogna – Consulenza per l'implementazione di Sistemi di Gestione Privacy:
svolgimento audit con clienti e redazione documentale ai sensi del Reg UE n.679/16 e d.lgs 196/2003, nonché supporto al cliente durante l'intero rapporto contrattuale.
Componente team DPO: audit, analisi e supporto sulla base dei compiti riservati al DPO
Consulenza per l'implementazione di Sistemi di Gestione della Sicurezza delle Informazioni - ISO 27001 (con estensioni 27017 e 27018):
Svolgimento di rating di cybersecurity
Supporto agli Organismi di Vigilanza nel settore socio-assistenziale/sanitario (d.lgs 231/20021)

Dott. Stefano Carlesso - Data Protection Officer e consulente privacy sulla protezione dei dati personali
Gestione di clienti in diversi ambiti (B2B, B2C, scuole, RSA e studi professionali) su tutto il territorio nazionale per quanto riguarda l'aspetto legato alla documentazione privacy, analisi preliminare, redazione documentale, supporto e consulenza.
Formazione del personale aziendale compresa la realizzazione del materiale formativo. Svolgimento di attività DPO

PROGRAMMA

L'evoluzione quantitativa del crimine informatico è ormai una sorta di certezza scontata (siamo sempre più connessi, usiamo sempre più dispositivi e le aziende sono sempre più digitalizzate), mentre l'evoluzione qualitativa continua ad assumere ritmi e connotati difficilmente pronosticabili.

Se in passato le offensive avevano un carattere generalizzato e diffuso, ora gli attacchi alla supply chain risultano sempre più spinti da spionaggio o sabotaggio di specifici target. A preoccupare è in particolare lo sfruttamento delle Pmi come cavalli di Troia, ossia come vettori di secondo grado. Ad esempio, anziché aggredire direttamente la grande azienda automotive si attacca il fornitore di componentistica con l'obiettivo di creare dei varchi indiretti (piattaforme di collaborazione, canali e-mail e altro). Le grandi imprese hanno iniziato da tempo a investire per ridurre gli attacchi informatici diretti, quindi gli attaccanti hanno dirottato la loro attenzione sulle pmi che hanno contatti diretti con le grandi aziende all'interno delle filiere.

L'offensiva di filiera sarà purtroppo in buona compagnia di altre tendenze preoccupanti, a partire dalla cosiddetta "doppia estorsione". Da scintilla dell'attacco, il ransomware (il virus informatico che chiede il riscatto del dispositivo) si sta trasformando nell'epilogo dell'offensiva. Tradotto: prima l'obiettivo era semplicemente bloccare il dispositivo e trarne un profitto tramite la richiesta di riscatto, mentre adesso i criminali si incuneano nei sistemi informatici, "rapiscono" i dati togliendoli dalla disponibilità dell'azienda e solo allora attivano il ransomware.

Così facendo, i criminali si garantiscono due leghe di estorsione: minacciare la pubblicazione dei dati sul mercato nero o sul web in caso di mancato pagamento del riscatto, oppure chiedere il pagamento per riavere indietro i dati. Se questa tecnica fa scorrere i brividi nella schiena dei responsabili della sicurezza informatica,

chissà cosa può provocare la tripla estorsione. Ancora una volta è l'innovazione a stupire: una volta entrati all'interno della rete aziendale, i criminali informatici impediscono all'azienda di usarla e nel frattempo la utilizzano indisturbati per attaccare terze parti. O meglio minacciano di farlo, perché prima c'è sempre la richiesta di riscatto e il movente è sempre economico.

Come se non bastasse, c'è da aggiungere al rapimento e alle estorsioni una terza tendenza: la "democratizzazione" dei malware. Prima chi creava malware era una sorta di artista, uno stregone del crimine informatico. Adesso è più che altro una disciplina alla portata di molti: chi sviluppava malware ha iniziato tra il 2017 e il 2018 a venderli come veri e propri servizi. Ormai basta comprarne uno, fornire un indirizzo e-mail e l'attacco è attivato.

L'altro problema è che questa industria progredisce anche in termini di innovazione. Il risultato è che il 76% dei software malevoli (da qui malware, abbreviazione di "malicious software") sono malware zero-day, ossia mai rilevati prima, e malware appena studiati, che come tali hanno una possibilità non trascurabile di aggirare i tradizionali perimetri di sicurezza.

In generale, e-mail e posta elettronica certificata sono ancora i vettori di attacco preferiti, soprattutto verso industria e banche italiane.

Vi è, infine, da mettere in evidenza un'altra tendenza, ossia la "propagazione laterale": anziché entrare da un unico punto di accesso, i criminali laterali cercano sempre più spesso di infettare più macchine e disponibili possibili, così da garantirsi più porte d'ingresso e quindi anche più tempo per girare e agire indisturbati. Il grande problema è la prospettiva: queste e altre metodologie stanno infatti iniziando a minacciare i settori più vulnerabili in termini di maturità informatica e resilienza di rete.

In Italia gli attacchi informatici sono aumentati di oltre il 250% nel secondo trimestre 2021 rispetto ai primi tre mesi del 2021 facendo registrare un preoccupante picco nel mese di giugno. L'emergenza Covid-19 ha influenzato pesantemente la sicurezza informatica in Italia. L'aumento dei lavoratori in smart working ha creato un campo fertile per il cybercrime.

La maggior parte degli attacchi sono collegabili all'emergenza coronavirus con oltre il 60% degli episodi che ha provocato il furto dei dati degli utenti. Tramite le tecniche di phishing i cybercriminali sono riusciti ad aggirare le difese degli utenti mettendo a segno numerosi furti di dati personali e facendo aumentare del 361% il numero di questi attacchi rispetto al primo trimestre del 2020. Questa tipologia di attacco ha superando di gran lunga sia le violazioni della privacy (11% dei casi) sia gli attacchi finalizzati alla sottrazione di denaro (7%).

Il trend per il 2022 è di ulteriore crescita degli attacchi.

DESTINATARI

A tutti i dipendenti dell'Ateneo che si trovino ad usare i pc ed internet. Sono le figure base ddell'Ente che non rivestono ruoli particolari in ambito IT.

ARGOMENTI TRATTATI

Panoramica sugli attacchi informatici (cyber risk)

- Obiettivi della cybersecurity
- Strutture di rete

- Uso delle credenziali (password)
- Regole per l'utilizzo di mail e strumenti informatici
- Phishing
- Malware
- Smartworking
- Social Eneneering e i rischi nella diffusione dei dati personali
- Utilizzo consapevole dei devices
- Reti wi-fi
- ISO 27001

Modalità di iscrizione e di recesso

L'iscrizione, comprensiva di materiali didattici, attestato e assistenza telematica per quesiti, è prevista al costo di

- **€200,00 Iva esente** (per la PA) a partecipante, oltre Iva 22% per tutti gli altri soggetti
- **Scontistica in abbonamento:** €180,00 Iva esente (per la PA) a partecipante https://www.lineapa.it/abbonamento-scontato-formazione-2022-lineatenei

Sono a carico dei partecipanti eventuali commissioni bancarie.

L'iscrizione si perfeziona tramite invio della scheda di adesione, a cui seguirà l'emissione di fattura elettronica.

È necessario compilare in tutte le parti la scheda di adesione presente in ultima pagina e trasmetterla via mail al seguente indirizzo: info@lineatenei.it o via fax al numero: 0125-5545190 **entro la data indicata sulla stessa.**

La cancellazione dell'iscrizione deve avvenire per iscritto a info@lineatenei.it e **non comporta addebiti se avviene entro 7 giorni dall'inizio dell'evento**. È sempre possibile sostituire l'iscritto impossibilitato a partecipare con un collega, anche il giorno stesso dell'incontro. In caso di impossibilità a partecipare sarà possibile, contattando entro le 48 ore antecedenti l'inizio dell'evento la segreteria a mezzo posta elettronica, concordare il trasferimento dell'iscrizione a una edizione successiva dell'evento o ad un'altra iniziativa di LineATENEI. In tutti gli altri casi la quota di iscrizione è dovuta interamente e si procederà all'emissione della fattura.

CONDIZIONI DI ADESIONE e EVENTUALI MODIFICHE

I corsi e le giornate di studio si svolgeranno nei luoghi e nelle ore indicate nella scheda di presentazione del corso e sul sito internet.

LineATENEI potrà in ogni caso modificare i luoghi, le date e gli orari del corso, così come annullare l'iniziativa previa comunicazione, telefonica e scritta al cliente; in tal caso il cliente, in sostituzione del rimborso della quota eventualmente già versata potrà richiedere di partecipare all'edizione successiva, se prevista o ad altro corso, salvo conguaglio.

LineATENEI in ogni caso non sarà tenuta a rimborsare al cliente null'altro che l'eventuale quota già versata non assumendosi alcuna responsabilità per eventuali costi aggiuntivi sostenuti dal cliente (prenotazioni alberghiere, spese di trasporto ecc..)

Essa, inoltre, si riserva in ogni momento e senza preavviso, di apportare modifiche al calendario dei lavori di ciascuna iniziativa pur garantendo il rispetto delle tematiche indicate nella scheda di presentazione del corso, così come di apportare modifiche alla composizione del corpo docente senza che da ciò derivi alcun diritto alla restituzione del corrispettivo da parte del cliente. Al pari la mancata partecipazione al corso o a singole lezioni non darà diritto alla restituzione del corrispettivo.

La conferma di svolgimento del corso verrà inviata in ogni caso alla mail di ogni iscritto non appena il numero di iscritti ne consente la realizzazione. Per eventuali informazioni aggiuntive, è possibile contattare i riferimenti in calce.

SCHEDA DI ADESIONE da inviare a info@lineatenei.it oppure al n° di fax 0125-5545190 entro il 2 Novembre 2022

Corso di formazione Cybersecurity base

Mercoledì 9 novembre 2022 orario **9:00 – 13:00**

Docenti: Dott.ssa Giulia Gradogna - Dott. Stefano Carlesso

Webinar online

Costo:

- **€200,00 Iva esente** (per la PA) a partecipante, oltre Iva 22% per tutti gli altri soggetti
- **Costo per gli enti in abbonamento:** €180,00 Iva esente (per la PA) a partecipante, https://www.lineapa.it/abbonamento-scontato-formazione-2022-lineatenei

La fattura elettronica verrà emessa da LineATENEI sas (dati in calce nella carta intestata)

Ente a cui deve essere intestata la fattura* _____

Via_____ **CAP**_____ **Città**_____

Codice fiscale_____ **P.IVA** _____ **Codice Univoco Ufficio***_____

Buono d'ordine o DG n° _____del _____di importo pari a €_____

CIG: _____ altro_____

Nome e Cognome del partecipante	**Cell o tel diretto**	**E mail**	**Ruolo**

Modalità di pagamento:

- Bonifico Bancario (anticipato per i privati) sul seguente c.c. intestato a **LineATENEI sas di Patrizia Isaija** IBAN: **IT75U0853031050000000013437** - Banca d'Alba, Filiale di Strambino (TO)

Informativa privacy: ai sensi dell'art. 13, D.Lgs 196/2003, i dati acquisiti sono utilizzati al fine di espletare il servizio in oggetto e per la promozione delle future iniziative di LineATENEI, titolare del trattamento. I dati forniti saranno inseriti nelle ns. banche dati e saranno trattati esclusivamente da ns. personale e dal personale esterno addetto alla contabilità. Per i diritti riservati all'interessato dalla legge, si rimanda all'art. 7, D.Lgs 196/2003. Il Responsabile del trattamento è la dottoressa Patrizia Isaija con cui è possibile comunicare scrivendo a info@lineatenei.it. Si dichiara di aver preso visione dell'informativa ex D.Lgs 196/2003 e si acconsente al trattamento dei dati nei limiti della stessa.

Data_____ Firma e timbro _____*Campi obbligatori

LineATENEI s.a.s. di Patrizia Isaija
CF e P.IVA 12398000013 - REA: 1287388
sede legale: - Via Roma 366 10121 Torino (c/o Studio Scarabosio e Lanteri)
sede operativa: Via Marconi 41 10010 Andrate (TO)
tel: 328.0365662 fax: 0125.5545190 e mail: info@lineatenei.it - pec: lineatenei@pec.it