



Unità Formativa 2: La sicurezza digitale nel turismo

Tourism Resilience Education in Digital Security



Co-funded by
the European Union

INDICE

INTRODUZIONE.....	3
UNITÀ DI FORMAZIONE 2: LA SICUREZZA DIGITALE NEL TURISMO.....	4
Obiettivi del corso	4
Risultati di apprendimento.....	4
Struttura e metodologia dell'unità	5
2.1 Fondamenti della sicurezza digitale	7
1. Perché la sicurezza digitale è fondamentale nel turismo	7
2. Concetti fondamentali di cybersecurity.....	11
3. Igiene informatica negli ambienti di lavoro del settore turistico.....	14
4. Fattore umano, ingegneria sociale e disinformazione	18
5. Fondamenti normativi: GDPR e NIS2 nel settore turistico	23
6. Ruoli, responsabilità e procedure di escalation.....	26
7. La sicurezza digitale nelle attività quotidiane del settore turistico	30
8. Verifica delle conoscenze ed esercitazioni.....	34
2.2 La sicurezza nei processi digitali del turismo	42
1. Processi digitali nel turismo e punti di rischio	42
2. Gestione sicura dei dati dei clienti	48
3. Pagamenti, frodi e truffe nelle prenotazioni	52
4. Esercitazione basata su uno scenario: pagamento sospetto	56
5. Le prime 24 ore dopo una violazione dei dati.....	58
6. Cooperazione con il reparto IT e i fornitori esterni	63
7. Tecnologie avanzate per la sicurezza digitale nel turismo.....	65
8. Riflessione e consolidamento	69
2.3 Simulazioni e gestione delle crisi digitali.....	73
1. Tipologie di incidenti digitali nel settore turistico	73
2. Pressione psicologica durante le crisi digitali	75
3. Caso studio 1 – Attacco ransomware al PMS di un hotel	77
4. Caso studio 2 – Campagna di phishing attraverso una piattaforma di prenotazione	80

Unità di Formazione 2: La sicurezza digitale nel turismo

5. Comunicazione di crisi.....	82
6. Recupero post-incidente e ricostruzione della fiducia	86
7. Discussione finale e valutazione	88
RIFERIMENTI	94

ELENCO DELLE FIGURE

Figura 1: Flusso di dati nel turismo e vulnerabilità tra OTA, CRS, PMS e sistemi di pagamento	9
Figura 2: Catena di un attacco di ingegneria sociale	19
Figura 3: Principali fasi di risposta nelle prime 24 ore dopo una violazione dei dati	60

Il progetto TREADS risponde all'accelerazione della trasformazione digitale del settore turistico europeo, con particolare attenzione alle micro-PMI e alle PMI che costituiscono la spina dorsale del settore. Sebbene la digitalizzazione migliori competitività ed efficienza operativa, introduce anche rischi significativi legati alla gestione dei dati, alla cybersecurity e alla disinformazione. Il settore turistico è tra i settori più presi di mira negli attacchi informatici, evidenziando l'urgente necessità di un'educazione e formazione strutturate che rafforzino la resilienza digitale.

Allo stesso tempo, il Patto UE per le Competenze per il Turismo (Pact for Skills) individua un persistente divario di competenze all'interno del settore, specialmente tra le piccole imprese del settore, dove le competenze digitali e di cybersecurity rimangono sviluppate in modo diseguale. Affrontare questa lacuna è essenziale per garantire una transizione sicura e sostenibile verso l'era digitale.

In questo contesto, il presente deliverable costituisce il curriculum formativo strutturato dell'Unità di Formazione 2: *La sicurezza digitale nel turismo* ed è progettato per essere erogato come un corso di 48 ore nell'ambito della formazione professionale (IeFP). Il corso è incentrato sulla sicurezza digitale nel turismo e affronta i processi digitali del settore turistico e la gestione delle crisi digitali attraverso una combinazione di basi teoriche, conoscenze del quadro normativo, esercitazioni pratiche e apprendimento basato su simulazioni. È allineato ai principali quadri strategici e normativi dell'Unione europea e mira a fornire a formatori e studenti dell'istruzione e formazione professionale competenze pratiche per rafforzare la resilienza organizzativa, promuovere pratiche digitali responsabili e garantire una risposta strutturata alle crisi all'interno dell'ecosistema turistico.

UNITÀ DI FORMAZIONE 2: LA SICUREZZA DIGITALE NEL TURISMO

Obiettivi del corso

Questa unità di formazione mira a rafforzare la capacità dei professionisti del turismo di operare in modo sicuro in ambienti digitalmente interconnessi. Fornisce conoscenze strutturate, competenze operative applicate e una consapevolezza orientata alla governance necessarie per gestire i rischi digitali nei processi turistici.

L'unità si propone di:

- Aumentare la consapevolezza dei rischi digitali sistemici all'interno di ecosistemi turistici interconnessi;
- Rafforzare le pratiche operative sicure nella gestione dei dati dei clienti, dei pagamenti e dei sistemi di prenotazione;
- Allineare il comportamento professionale alle politiche di sicurezza organizzative e ai requisiti normativi dell'UE;
- Rafforzare procedure strutturate di escalation e risposta coordinata agli incidenti;
- Favorire la resilienza digitale e mantenere la fiducia dei clienti nelle imprese del settore turistico.

L'obiettivo più ampio di questa unità è supportare lo sviluppo di professionisti del turismo digitalmente competenti che combinino la consapevolezza tecnica con un comportamento responsabile e una risposta strutturata agli incidenti.

Risultati di apprendimento

CONOSCENZE

Al termine della formazione, lo studente sarà in grado di descrivere i concetti di base della sicurezza digitale e di comprendere le principali minacce informatiche che interessano il settore turistico. Saprà riconoscere le vulnerabilità più comuni nei processi digitali del turismo, come i sistemi di prenotazione online, i pagamenti digitali e le pratiche di gestione dei dati. Comprenderà inoltre i principi fondamentali della sicurezza digitale, incluso il concetto di Zero Trust Security, e sarà in grado di identificare i principali requisiti normativi in materia di protezione dei dati e sicurezza digitale, come il Regolamento Generale sulla Protezione dei Dati (GDPR). Infine, comprenderà in che modo gli incidenti digitali possono influire sulla continuità operativa e sulla reputazione delle organizzazioni turistiche.

ABILITA'

Lo studente sarà in grado di applicare pratiche di base di sicurezza digitale nelle attività quotidiane del turismo e di seguire procedure sicure nella gestione dei dati dei clienti, delle prenotazioni online e dei sistemi di pagamento digitali. Saprà individuare e segnalare attività digitali sospette, come tentativi di phishing o frodi online, e reagire in modo appropriato a incidenti informatici simulati, inclusi violazioni dei dati o attacchi ransomware. Inoltre, sarà in grado di contribuire alle procedure interne di comunicazione e risposta durante situazioni di crisi digitale.

COMPETENZE

Lo studente opererà in modo responsabile nell'utilizzo dei sistemi digitali e dei dati dei clienti, nel rispetto delle politiche di sicurezza adottate dall'organizzazione. Sarà in grado di supportare la risposta dell'organizzazione agli incidenti di sicurezza digitale, entro il proprio livello di responsabilità, e di adattare comportamenti e procedure per ridurre i rischi digitali negli ambienti turistici.

Struttura e metodologia dell'unità

DURATA

48 ore (16 per ogni sottounità)

METODI DI EROGAZIONE

L'unità può essere erogata online, tramite apprendimento individuale o di gruppo, oppure in presenza.

ATTIVITÀ PRATICHE E RISULTATI CORRELATI

- Valutazione di base della sicurezza di un sito web turistico, finalizzata all'individuazione di potenziali vulnerabilità legate alla protezione dei dati, alle prenotazioni online e alla gestione degli accessi degli utenti. Al termine dell'attività verrà redatto un breve report sulla sicurezza, contenente i rischi individuati e le relative misure di mitigazione consigliate;
- Caso studio su un attacco ransomware a un sistema di gestione alberghiero (Property Management System – PMS). Gli studenti analizzeranno un caso realistico, concentrandosi sulle cause dell'incidente, sugli impatti operativi e reputazionali e sulle azioni di risposta adottate, producendo un'analisi scritta del caso che descriva l'evento, la strategia di gestione e le lezioni apprese;
- Workshop sulla pianificazione della comunicazione in caso di violazione dei dati: attraverso il lavoro di gruppo, gli studenti progettano e redigono un piano di comunicazione per la gestione della comunicazione interna ed esterna durante una fuga di dati o un incidente di sicurezza digitale, presentando poi il lavoro al formatore e agli altri partecipanti;
- Simulazioni di attacchi di phishing e di frodi nelle prenotazioni online, seguite dalla compilazione di una checklist che documenti le risposte corrette adottate e le aree di miglioramento individuate;
- Sviluppo di un piano completo di sicurezza digitale per un'agenzia di viaggi o una struttura alberghiera, comprendente misure preventive, procedure di risposta agli incidenti e la definizione di ruoli e responsabilità.

Le attività pratiche possono essere svolte individualmente o in gruppo, a seconda del contesto.

VALUTAZIONE

- Brevi quiz sulla conoscenza teorica;
- Valutazione delle attività pratiche attraverso, ad esempio, questionari, quiz, hackaton, relazioni, checklist e presentazioni di gruppo.

Il raggiungimento degli obiettivi di apprendimento sarà valutato sulla base della capacità dei partecipanti di riconoscere correttamente i rischi legati alla sicurezza digitale in scenari pratici collegati al settore turistico. Agli studenti sarà richiesto di dimostrare un uso sicuro degli strumenti digitali durante simulazioni o attività pratiche, nonché di superare esercitazioni di individuazione di phishing o frodi.

La valutazione terrà inoltre conto del contributo alla progettazione di un semplice piano di risposta a incidenti digitali o di comunicazione. Infine, i partecipanti dovranno superare prove finali che integrano conoscenze teoriche e applicazione pratica.

2.1 Fondamenti della sicurezza digitale

Alla fine della sottounità, i partecipanti saranno in grado di riconoscere comportamenti digitali non sicuri, applicare regole di sicurezza di base nel lavoro quotidiano, segnalare correttamente gli incidenti e comprendere ruoli e responsabilità.

- Concetti di base della sicurezza digitale:
 - Igiene informatica (gestione password, autenticazione a più fattori – MFA, aggiornamenti, backup);
 - Il fattore umano nella sicurezza digitale;
 - Quadro normativo (nozioni di base sul GDPR per il personale turistico), Direttiva NIS2 (panoramica e rilevanza per la filiera turistica);
- Le minacce digitali più comuni nel settore turistico;
- Disinformazione e social engineering (ingegneria sociale) rivolte alle aziende turistiche (recensioni false, falsi allarmi, comunicazioni con i clienti manipolate);
- Introduzione alla sicurezza Zero Trust.

Attività pratica suggerita:

- Quiz di consapevolezza sulla sicurezza digitale

1. Perché la sicurezza digitale è fondamentale nel turismo

La sicurezza digitale svolge un ruolo fondamentale nel settore turistico, in cui le organizzazioni raccolgono ed elaborano costantemente dati personali e di pagamento all'interno di ambienti digitali interconnessi. I sistemi di prenotazione, le piattaforme online e i servizi di pagamento si scambiano dati in tempo reale per

consentire prenotazioni, check-in e transazioni finanziarie. Gli elevati volumi di transazioni, l'ampio ricorso a partner esterni e la continua disponibilità dei sistemi ampliano significativamente la superficie di attacco, aumentando l'esposizione a errori operativi, usi impropri e attacchi informatici. Poiché questi sistemi sono strettamente interconnessi, anche una piccola vulnerabilità in una parte della catena digitale può avere conseguenze rilevanti per gli ospiti, il personale e la continuità operativa dell'organizzazione.

I principali sistemi coinvolti in questo flusso di dati comprendono:

- **Property Management System (PMS)** – sistemi interni delle strutture ricettive utilizzati per gestire prenotazioni, check-in, registrazione degli ospiti e fatturazione;
- **Central Reservation System (CRS)** – sistemi che sincronizzano la disponibilità delle camere e le tariffe tra i diversi canali di prenotazione;
- **Piattaforme di pagamento** – strumenti utilizzati per elaborare pagamenti con carta, rimborsi e storni (chargeback).

Poiché questi sistemi sono interconnessi, una vulnerabilità in uno di essi può compromettere il funzionamento degli altri. Un incidente tipico segue generalmente una sequenza prevedibile:



Ad esempio, in casi reali, alcune strutture ricettive che hanno continuato ad accettare pagamenti senza il sistema **3-D Secure** (un ulteriore livello di verifica dell'identità del titolare della carta) durante gravi interruzioni dei sistemi hanno successivamente registrato un aumento degli storni (chargeback) e delle perdite finanziarie. Questo rischio spiega perché la normativa dell'Unione europea in materia di condivisione affidabile dei dati e responsabilità, in particolare il Data Governance Act¹, promuove meccanismi volti a facilitare la condivisione dei dati tra

¹ Parlamento europeo e Consiglio dell'Unione europea. (2022). *Regolamento (UE) 2022/868 del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Data Governance Act – Legge sulla governance dei dati)*. Gazzetta ufficiale dell'Unione Europea. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R0868>

i diversi settori, rafforzando al contempo la fiducia nelle modalità di gestione dei dati.

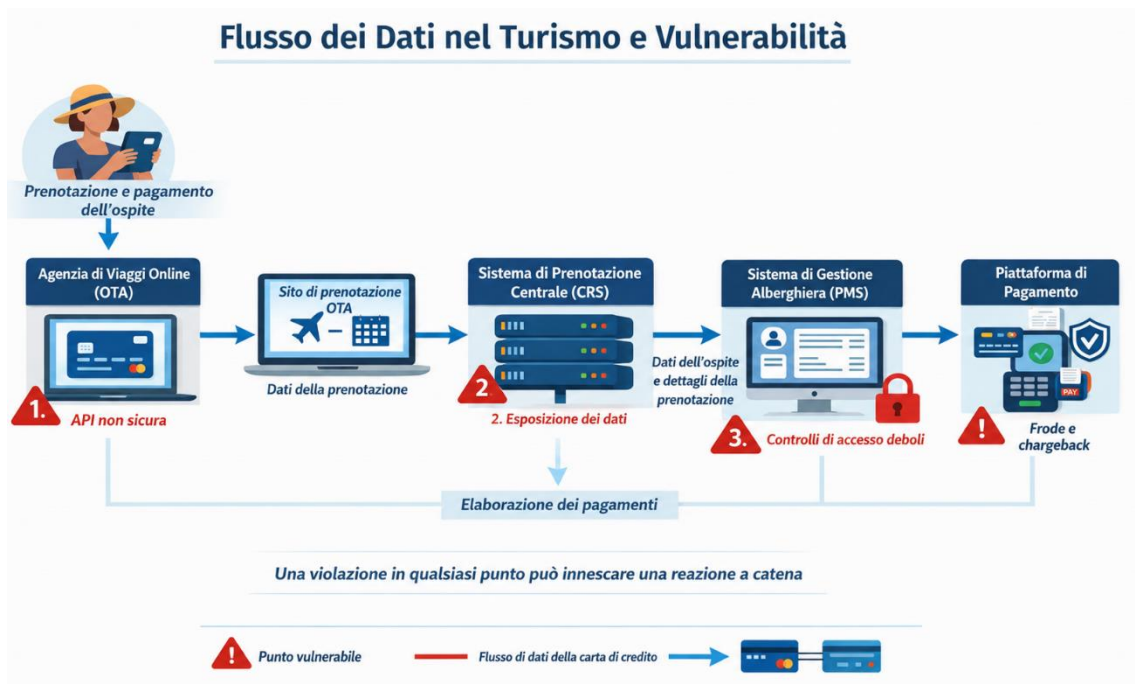


Figura 1: Flusso di dati sul turismo e vulnerabilità tra OTA, CRS, PMS e sistemi di pagamento

Il settore turistico è particolarmente esposto perché i dati vengono costantemente condivisi tra diversi soggetti. Un'unica **API** esposta — un'interfaccia digitale che consente a differenti sistemi software di comunicare tra loro — all'interno di un'**agenzia di viaggi online (Online Travel Agency – OTA)** può permettere ai truffatori di accedere a grandi volumi di dati relativi alle prenotazioni. Una volta ottenuto un punto di accesso, gli aggressori possono propagarsi attraverso i sistemi collegati, provocando effetti a catena che coinvolgono più organizzazioni. La dimensione etica della protezione dei viaggiatori e dei loro dati è esplicitamente evidenziata anche nel **Codice etico globale per il turismo dell'UNWTO²**, che afferma come *"i soggetti pubblici e privati coinvolti nello sviluppo del turismo dovrebbero cooperare nell'attuazione di tali principi"*, sottolineando l'importanza della cooperazione e della responsabilità condivisa nella loro applicazione.

Questi incidenti producono conseguenze concrete. Gli ospiti possono essere vittime di frodi o di utilizzo illecito della propria identità; il personale è costretto a dedicare

² Organizzazione Mondiale del Turismo (UNWTO). (s.d.). *Codice etico globale per il turismo*. <https://www.untourism.int/global-code-of-ethics-for-tourism>

tempo alla gestione degli incidenti anziché all'assistenza dei clienti; inoltre, le organizzazioni subiscono danni economici e reputazionali. La responsabilità etica di proteggere gli ospiti è ribadita anche dal *Codice etico globale per il turismo* dell'UNWTO, secondo cui gli operatori del settore turistico dovrebbero garantire la tutela dei turisti e dei loro dati personali.

Per approfondire

I rischi per la sicurezza digitale variano a seconda del modello di business:

- **Le strutture ricettive** si concentrano sulla protezione dei dati degli ospiti, generalmente archiviati in sistemi centralizzati, e sul mantenimento della continuità delle operazioni quotidiane. Gli incidenti hanno spesso un impatto operativo immediato, compromettendo attività quali il check-in, la fatturazione e l'esperienza complessiva degli ospiti.
- **Le Destination Marketing Organizations (DMO)** si basano su banche dati condivise e flussi informativi provenienti dai partner. Ciò le rende vulnerabili a dati corrotti, ritardati o fuorvianti, con possibili ripercussioni sulla reputazione della destinazione e sui processi decisionali.
- **Le agenzie di viaggio online (OTA)** centralizzano le prenotazioni di migliaia di fornitori e integrano numerosi partner attraverso interfacce tecniche. Sono particolarmente esposte al rischio sistemico legato alle API, in cui una singola vulnerabilità può propagarsi simultaneamente a più organizzazioni.

Affrontare questi rischi richiede lo sviluppo delle competenze della forza lavoro e il rafforzamento delle competenze digitali. A tal fine, il partenariato per le competenze nel settore del turismo, promosso nell'ambito del Patto per le Competenze (Pact for Skills) dell'Unione europea, mira a favorire l'aggiornamento (upskilling) e la riqualificazione (reskilling) del 60% della forza lavoro ogni anno entro il 2030 in tutto l'ecosistema turistico³. Tale iniziativa contribuisce direttamente a rafforzare la consapevolezza in materia di cybersecurity e la resilienza operativa.

³ Commissione europea. (2024). *Il Patto per le Competenze dell'UE – Partenariato per le competenze dell'ecosistema del turismo (Aggiornamento della baseline)*. Commissione Europea. https://pact-for-skills.ec.europa.eu/document/download/83968c43-1706-4fbd-9fd0-4461583607d7_en?filename=Pact%20for%20Skills%20Tourism%20Baseline%20-%20update%2020240229.pdf

Riflessione e discussione

01

Perché il settore turistico è considerato un settore ad alto rischio dal punto di vista della sicurezza digitale?

02

Indica due possibili conseguenze di un incidente digitale e spiegate una.

03

Per approfondire: quale modello di business è maggiormente esposto ai rischi derivanti da API non sicure e perché?

2. Concetti fondamentali di cybersecurity

Il rischio per la sicurezza digitale segue una logica semplice e ricorrente, comune alla maggior parte delle organizzazioni e dei sistemi. Nella maggior parte dei casi, i truffatori iniziano individuando vulnerabilità comuni e facilmente sfruttabili, piuttosto che ricorrere a tecniche altamente sofisticate. Tra gli esempi più frequenti vi sono password deboli o riutilizzate, configurazioni errate dei sistemi e mancati aggiornamenti del software.

Quando una di queste vulnerabilità viene sfruttata, l'impatto raramente rimane confinato a un singolo sistema. Le conseguenze possono rapidamente includere la perdita di dati personali o aziendali, l'interruzione dei servizi, frodi finanziarie e ulteriori costi di ripristino legati alle attività di indagine, risoluzione dell'incidente e perdita di produttività. Comprendere questa relazione di causa-effetto è essenziale per riconoscere come piccole vulnerabilità possano trasformarsi in gravi problemi operativi e aziendali.

Negli ambienti turistici, i rischi generalmente rientrano in due **categorie strettamente interconnesse**:

- **Rischi tecnici**, come interfacce di sistema (API) non sicure, server obsoleti, servizi configurati in modo inadeguato e mancata applicazione delle patch di sicurezza.
- **Rischi legati al fattore umano**, quali attacchi di phishing, uso improprio delle credenziali o divulgazione accidentale di dati personali.

Questi rischi si rafforzano reciprocamente. Ad esempio, una singola e-mail di phishing può indurre un membro del personale a rivelare le proprie credenziali, consentendo così a un truffatore di sfruttare una vulnerabilità tecnica già esistente.

Allo stesso modo, un malfunzionamento tecnico può generare confusione o un senso di urgenza, condizioni che i truffatori possono sfruttare per manipolare il comportamento delle persone.

Zero Trust come principio pratico di sicurezza

Per ridurre la diffusione degli incidenti informatici, uno dei principi di sicurezza più diffusi è lo **Zero Trust**. Anziché presumere che utenti o sistemi siano affidabili per impostazione predefinita, l'accesso viene concesso solo dopo un'adeguata verifica. Gli elementi fondamentali di questo approccio comprendono la verifica dell'identità, la limitazione degli accessi allo stretto necessario, la separazione dei sistemi ove possibile e il monitoraggio delle attività per individuare eventuali anomalie.

Nella pratica, il modello Zero Trust contribuisce a garantire che la compromissione di un account o di un sistema non comporti automaticamente un accesso esteso a tutti gli ambienti interconnessi. Questo aspetto è particolarmente importante nel settore turistico, dove i sistemi sono fortemente integrati e i ruoli del personale cambiano frequentemente.

Misure pratiche di mitigazione

A questo livello, le misure di mitigazione più efficaci sono semplici da applicare e facilmente attuabili:

- applicare regolarmente gli aggiornamenti software e le patch di sicurezza, così da correggere le vulnerabilità note prima che possano essere sfruttate;
- utilizzare metodi di autenticazione robusti e applicare il principio del privilegio minimo, affinché ogni utente possa accedere esclusivamente ai sistemi e ai dati necessari per lo svolgimento del proprio ruolo;
- registrare e monitorare le attività sospette, mantenendo traccia delle principali operazioni eseguite sui sistemi e verificando la presenza di comportamenti anomali;
- formare il personale al riconoscimento degli attacchi di phishing e delle altre tecniche di ingegneria sociale (social engineering), in modo che messaggi o richieste sospette vengano individuati e segnalati tempestivamente.

Nel loro insieme, queste misure consentono di ridurre sia i rischi di natura tecnica sia quelli legati al fattore umano, contribuendo a limitare i danni qualora si verifichi un incidente.

Scenario: verifica dell'identità in una situazione di pressione

Una celebrità di fama internazionale soggiorna presso la vostra struttura. La reception riceve una telefonata da una persona che si presenta come "assistente personale" dell'ospite e richiede il numero della camera e una copia della scheda di check-in "per motivi fiscali".

Questa situazione solleva alcune importanti questioni:

- **Il dilemma:** applicare il principio dello Zero Trust significa diffidare di chiunque, anche a costo di rischiare di offendere un ospite VIP?
- **La sfida della collaborazione:** come può il personale verificare l'identità del chiamante attraverso le procedure previste, senza apparire scortese o compromettere l'esperienza dell'ospitalità?

Questo scenario evidenzia come i principi di sicurezza debbano essere applicati in modo da conciliare le esigenze di protezione con la cultura dell'accoglienza che caratterizza il settore turistico.

Per approfondire

Sebbene il modello Zero Trust sia molto efficace dal punto di vista concettuale, i sistemi più datati (legacy systems) spesso non dispongono di funzionalità integrate per la gestione delle identità o la segmentazione degli accessi. In questi contesti, le organizzazioni ricorrono a **misure di sicurezza compensative**, come l'autenticazione tramite gateway, la segmentazione della rete e un monitoraggio più approfondito delle attività di sistema (enhanced logging), per ridurre l'esposizione ai rischi. Pianificare un aggiornamento graduale dei sistemi, affiancato da misure di protezione temporanee, è essenziale per gestire efficacemente il rischio senza compromettere la continuità delle attività operative.

Lo Zero Trust deve quindi essere considerato un approccio strategico alla sicurezza di lungo periodo, piuttosto che una singola tecnologia o una soluzione rapida.

Riflessione e discussione

01

Qual è la differenza tra una minaccia e una vulnerabilità?

02

Fornisci due esempi di rischi legati al fattore umano e descrivi una semplice misura di mitigazione.

03

Per approfondire: qual è il principale limite nell'applicazione del modello Zero Trust ai sistemi legacy?

3. Igiene informatica negli ambienti di lavoro del settore turistico

La maggior parte degli incidenti digitali non inizia con un attacco sofisticato da parte di hacker, bensì con le normali attività quotidiane. I comportamenti adottati durante il lavoro influenzano in modo significativo la probabilità che piccoli problemi rimangano circoscritti o si trasformino in gravi incidenti informatici.

Tra gli errori più comuni nella routine lavorativa rientrano:

- utilizzare password deboli o riutilizzate (ad esempio, 123456 o password);
- rimandare o ignorare gli aggiornamenti del software;
- lasciare aperte le sessioni su dispositivi condivisi, ad esempio alla reception o negli uffici amministrativi;
- salvare le password nel browser su computer utilizzati da più persone;
- utilizzare reti Wi-Fi pubbliche non protette per attività lavorative.

Nelle organizzazioni turistiche, dove ogni giorno vengono trattati dati personali e informazioni di pagamento, anche queste apparentemente piccole disattenzioni possono provocare rapidamente esposizione dei dati, transazioni fraudolente o interruzioni dei servizi.

Misure pratiche ad alto impatto

Le misure pratiche ad alto impatto mirano a ridurre i rischi digitali quotidiani. Sono particolarmente efficaci quando sono semplici da applicare e vengono adottate con costanza. Più che fare affidamento su tecnologie avanzate, queste misure puntano sulla prevenzione e sulla limitazione tempestiva dei danni, rafforzando i

comportamenti quotidiani, il controllo degli accessi e le pratiche di base per la sicurezza dei sistemi.

Le principali misure includono:

- **Utilizzare password robuste e diverse per ciascun sistema** (ad esempio BlueCoffee-Flying-Moon!77) e conservarle in modo sicuro mediante un gestore di password (password manager). Le password dovrebbero essere cambiate immediatamente in caso di sospetta compromissione, dopo un incidente di sicurezza, quando vi sia il rischio che le credenziali siano state esposte oppure quando previsto dalle politiche dell'organizzazione. Il cambio periodico delle password, in assenza di evidenze di compromissione, è generalmente sconsigliato, poiché può favorire la scelta di password più deboli o il loro riutilizzo.
- **Abilitare l'autenticazione a più fattori (Multi-Factor Authentication – MFA)**, aggiungendo un ulteriore livello di protezione che impedisce la compromissione degli account anche nel caso in cui le password vengano sottratte.
- **Installare regolarmente gli aggiornamenti software e le patch di sicurezza**, così da correggere le vulnerabilità note prima che possano essere sfruttate.

Gestione dei rischi legati ai dispositivi condivisi e al lavoro da remoto

I dispositivi condivisi rappresentano un rischio specifico negli ambienti di lavoro del settore turistico, dove più membri del personale utilizzano gli stessi sistemi durante turni differenti. Poiché le attività di utenti diversi si sovrappongono, diventa più difficile attribuire le responsabilità e più facile che accessi non autorizzati passino inosservati.

Le **misure di mitigazione** più semplici ed efficaci includono:

- bloccare lo schermo quando si allontana da una postazione di lavoro;
- utilizzare un account utente personale per ogni membro dello staff;
- evitare la memorizzazione delle password nel browser del computer condivisi.

Il lavoro da remoto richiede ulteriori precauzioni. Il personale dovrebbe utilizzare reti affidabili oppure una **VPN** (Virtual Private Network) ed evitare le reti Wi-Fi pubbliche quando svolge attività che comportano il trattamento di informazioni sensibili.

Sicurezza dei dispositivi mobili nel settore turistico

I dispositivi mobili sono ormai parte integrante delle attività quotidiane nel settore turistico. Smartphone e tablet vengono spesso utilizzati dal personale per accedere alla posta elettronica, alle piattaforme di prenotazione, ai sistemi di pagamento, alle informazioni sui clienti e agli strumenti di comunicazione.

Se un dispositivo viene smarrito, rubato o compromesso, persone non autorizzate potrebbero accedere ai sistemi aziendali o a dati sensibili dei clienti. Per questo motivo, **i dispositivi mobili devono essere protetti con la stessa attenzione riservata ai computer e agli altri sistemi utilizzati sul luogo di lavoro.**

Tra le **buone pratiche** si raccomanda di:

- utilizzare un sistema di blocco dello schermo (PIN, password, impronta digitale o riconoscimento facciale);
- abilitare l'autenticazione a più fattori (MFA) quando disponibile;
- mantenere dispositivi e applicazioni costantemente aggiornati con le ultime patch di sicurezza e gli aggiornamenti software;
- scaricare app esclusivamente da fonti affidabili;
- segnalare tempestivamente lo smarrimento o il furto di un dispositivo;
- evitare di accedere a informazioni sensibili tramite reti Wi-Fi pubbliche non protette.

Anche semplici precauzioni possono ridurre significativamente il rischio di accessi non autorizzati e contribuire alla protezione sia delle informazioni dell'organizzazione sia dei dati dei clienti.

Sviluppare comportamenti sicuri attraverso la formazione

La formazione svolge un ruolo fondamentale nel trasformare le misure di sicurezza in abitudini consolidate. Il personale deve comprendere in che modo gli attacchi di

phishing e le tecniche di ingegneria sociale sfruttano i comportamenti quotidiani, come fare clic su un link o inserire le proprie credenziali sotto pressione.

Una formazione efficace dovrebbe concentrarsi su:

- riconoscere messaggi e richieste sospetti;
- sapere quando e come segnalare un potenziale incidente;
- esercitarsi nelle procedure di escalation, affinché i problemi vengano affrontati rapidamente.

Nel loro insieme, queste misure pratiche riducono in modo significativo la probabilità che un singolo errore, come fare clic su un collegamento malevolo o lasciare aperta una sessione, si trasformi in un grave incidente capace di arrecare danni agli ospiti o di compromettere il regolare svolgimento delle attività del personale.

Metodi di autenticazione emergenti: le passkey

Le passkey rappresentano un metodo di autenticazione emergente progettato per sostituire le tradizionali password. Aniché basarsi su credenziali da memorizzare, le passkey utilizzano chiavi crittografiche archiviate in modo sicuro su un dispositivo affidabile e vengono generalmente sbloccate tramite dati biometrici (ad esempio l'impronta digitale o il riconoscimento facciale) oppure mediante il PIN del dispositivo.

I **principali vantaggi** includono:

- maggiore resistenza agli attacchi di phishing;
- eliminazione del riutilizzo delle password;
- migliore esperienza utente;
- maggiore protezione contro la compromissione degli account (account takeover).

I principali fornitori di tecnologie digitali, come Apple, Google e Microsoft, supportano sempre più l'utilizzo delle passkey sia nei servizi destinati ai consumatori sia nelle soluzioni aziendali. Con la loro progressiva diffusione, anche le organizzazioni del settore turistico potranno adottare l'autenticazione tramite

passkey nei sistemi di prenotazione, nelle piattaforme cloud e nelle applicazioni rivolte ai clienti.

Per approfondire

La definizione delle politiche di sicurezza deve trovare un equilibrio tra protezione e praticità. Regole eccessivamente rigide o complesse, come l'obbligo di cambiare continuamente la password o procedure di autenticazione troppo onerose per attività di routine, possono ridurre l'adesione del personale alle misure di sicurezza. Al contrario, controlli troppo permissivi aumentano l'esposizione ai rischi. L'approccio più efficace consiste nell'adottare misure di sicurezza mirate, prevedere eccezioni chiaramente definite e stabilire procedure semplici e facilmente applicabili, affinché il personale possa integrare comportamenti sicuri nella propria attività quotidiana in modo naturale e costante.

Riflessione e discussione

01

Quali tre azioni di routine contribuiscono maggiormente a ridurre il rischio di compromissione di un account e perché?

02

Indica un rischio associato all'utilizzo di dispositivi condivisi e una semplice misura di mitigazione.

03

Per approfondire: perché una politica di igiene informatica deve trovare un equilibrio tra sicurezza e praticità?

4. Fattore umano, ingegneria sociale e disinformazione

Gli attacchi che sfruttano il fattore umano fanno leva sulla **fiducia** e sui **comportamenti abituali delle persone**, piuttosto che sulle vulnerabilità tecniche. E-mail di phishing, telefonate di impersonificazione e false richieste da parte di fornitori utilizzano messaggi credibili per indurre il personale a condividere credenziali di accesso, autorizzare pagamenti o divulgare informazioni sensibili. Negli ambienti del settore turistico, i truffatori si spacciano spesso per partner conosciuti, piattaforme di prenotazione o colleghi, creando un senso di urgenza per indurre il personale a bypassare le normali procedure di verifica.

La logica alla base di questi attacchi è semplice e ricorrente:



Figura 2: Catena di attacco di ingegneria sociale

Scenario pratico: richiesta urgente da parte di un fornitore

Il responsabile amministrativo di un hotel riceve un'e-mail che sembra provenire da un fornitore storico, nella quale viene richiesta con urgenza la modifica delle coordinate bancarie per il pagamento. Il messaggio utilizza un linguaggio familiare e include una fattura apparentemente autentica. Poiché la richiesta è contrassegnata come urgente e il mittente sembra affidabile, il responsabile avverte la pressione di agire rapidamente per evitare ritardi nei pagamenti.

Utilizza la checklist seguente per valutare la situazione:

- ✓ La richiesta è urgente o fa leva sulle emozioni?

- ✓ Riguarda denaro, accesso ai sistemi o dati sensibili?
- ✓ Il mittente sembra familiare e affidabile?
- ✓ La richiesta può essere verificata tramite un canale di contatto già noto e affidabile?
- ✓ È prevista una seconda approvazione o una conferma interna?
- ✓ La richiesta evita le normali procedure di approvazione o di verifica?
- ✓ Sono presenti piccole incongruenze (nomi, firme, numeri di fattura, formattazione)?
- ✓ Il messaggio esercita pressione affinché si agisca immediatamente, senza lasciare il tempo necessario per effettuare le verifiche?
- ✓ Se la richiesta fosse fraudolenta, quale sarebbe il potenziale impatto su denaro, dati o reputazione?

Disinformazione e ingegneria sociale nel turismo

La disinformazione aggiunge un ulteriore livello di rischio agli attacchi di ingegneria sociale. Falsi avvisi, recensioni online manipolate o messaggi contraffatti inviati a nome dei clienti possono indurre in errore sia il personale sia gli ospiti, provocare azioni non necessarie e compromettere la fiducia nei sistemi e nelle organizzazioni.

Tra i principali segnali di allarme di un tentativo di ingegneria sociale vi sono:

- linguaggio urgente o emotivamente coinvolgente;
- richieste inattese riguardanti pagamenti o accessi ai sistemi;
- indirizzi del mittente insoliti o non corrispondenti;
- piccole incoerenze nell'ortografia, nella formattazione o nel tono del messaggio.

La misura difensiva più efficace è **la verifica**. Le richieste sospette dovrebbero essere confermate attraverso un canale indipendente, ad esempio telefonando a un numero di contatto già conosciuto oppure verificando internamente con il personale competente. Per operazioni finanziarie o altre azioni sensibili, richiedere una seconda approvazione riduce in modo significativo il rischio.

Interrompere la catena dell'attacco

Procedure ben progettate possono interrompere tempestivamente gli attacchi di ingegneria sociale. Richiedere una verifica prima di eseguire qualsiasi operazione, separare le responsabilità (ad esempio affidando a persone diverse l'avvio e

l'approvazione di una transazione) e definire chiare procedure di escalation riducono drasticamente i potenziali danni. Questi controlli risultano efficaci anche senza modificare i sistemi tecnici esistenti.

Una cultura orientata alla verifica prudente, unita a semplici controlli sulle transazioni, rende molto più difficile per i truffatori trasformare un primo contatto in una frode o in una perdita di dati.

Esempio reale: attacco ransomware segnalato ai danni di una catena alberghiera europea⁴

Nell'ottobre 2023, il gruppo alberghiero europeo **Motel One** ha rivelato di essere stato colpito da un attacco ransomware attribuito al gruppo di **cybercriminali ALPHV/BlackCat**. Secondo quanto riportato da fonti pubbliche, l'incidente ha comportato **un accesso non autorizzato a dati relativi ai clienti, comprese informazioni sulle prenotazioni e dati di contatto** (SecurityWeek, 2023).

Sebbene l'azienda abbia dichiarato che le attività degli hotel sono proseguite regolarmente, l'attacco ha sollevato preoccupazioni riguardo alla possibile esposizione di dati personali e ha comportato implicazioni di natura normativa e reputazionale. Come avviene frequentemente negli attacchi ransomware, i truffatori hanno pubblicato online dichiarazioni riguardanti la presunta quantità di dati sottratti; tuttavia, tali affermazioni possono eccedere le informazioni ufficialmente confermate e dovrebbero essere interpretate con cautela durante lo svolgimento delle indagini.

Il caso dimostra come carenze nei controlli sugli accessi amministrativi e nella sicurezza della rete possano favorire un'esposizione su larga scala dei dati nel settore dell'ospitalità. Anche quando i servizi principali continuano a funzionare, un attacco ransomware può provocare interruzioni operative, perdite economiche, controlli da parte delle autorità competenti e danni reputazionali di lungo periodo.

Questo esempio evidenzia la natura sistemica del rischio digitale negli ecosistemi turistici, nei quali l'interconnessione tra sistemi di prenotazione, piattaforme di pagamento e sistemi CRM può amplificare l'impatto degli incidenti informatici sotto il profilo operativo, finanziario e normativo.

⁴ Security Week (October 2023). *Motel One Discloses Ransomware Attack Impacting Customer Data*. <https://www.securityweek.com/motel-one-discloses-ransomware-attack-impacting-customer-data/>

Ingegneria sociale potenziata dall'IA

Gli attacchi di ingegneria sociale sfruttano sempre più spesso l'intelligenza artificiale per creare comunicazioni fraudolente più convincenti e personalizzate. In passato, i messaggi di phishing erano spesso più facili da riconoscere perché contenevano errori ortografici, formulazioni insolite o altri segnali che ne mettevano in dubbio l'autenticità. Oggi, invece, gli strumenti basati sull'IA sono in grado di generare e-mail, messaggi, registrazioni audio e persino video dall'aspetto altamente professionale e molto simili a comunicazioni legittime.

- email di phishing generate dall'IA;
- attacchi di voice cloning (vishing), basati sulla clonazione della voce;
- impersonificazione tramite deepfake video;
- falsi messaggi di clienti generati da strumenti di IA;
- attacchi prompt injection rivolti ai sistemi di intelligenza artificiale utilizzati all'interno delle organizzazioni;

Queste tecniche rendono le verifiche più difficili, poiché i truffatori possono imitare persone o organizzazioni affidabili con un elevato grado di credibilità. Dirigenti, fornitori, colleghi, partner commerciali o clienti possono essere impersonati con l'obiettivo di ottenere informazioni, accedere ai sistemi o convincere il personale a compiere azioni che normalmente non eseguirebbe. Per questo motivo, le organizzazioni dovrebbero attribuire ancora maggiore importanza alle procedure di verifica e alla conferma indipendente delle richieste insolite, anche quando le comunicazioni sembrano autentiche.

Esempio reale: impersonificazione di dirigenti tramite deepfake⁵

Nel 2024 una multinazionale del settore dell'ingegneria è stata presa di mira da truffatori che hanno utilizzato la tecnologia deepfake durante una videoconferenza per impersonare alcuni dirigenti dell'azienda. Convinto che la riunione fosse autentica, un dipendente ha autorizzato una serie di transazioni che hanno provocato perdite per circa 25 milioni di dollari statunitensi (USD).

Per approfondire

⁵ CNN (2024). *Finance worker pays out \$25 million after video call with deepfake "chief financial officer"*. <https://edition.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk>

Analizzando la catena di un attacco di ingegneria sociale (ricognizione → contatto → sfruttamento → monetizzazione della frode), il punto in cui è possibile ottenere il maggiore effetto di protezione è rappresentato dalle fasi iniziali. Solide procedure di verifica dell'identità, rigorosi controlli per l'approvazione delle transazioni e passaggi obbligatori di conferma limitano in modo significativo la libertà di azione dei truffatori e riducono le conseguenze delle fasi successive dell'attacco. Queste misure rimangono efficaci anche quando non è ancora possibile effettuare un completo aggiornamento delle infrastrutture tecnologiche.

Riflessione e discussione

01

Quali tattiche usano i truffatori per ingannare il personale e qual è una conseguenza diretta?

02

Indica due segnali di allarme di un messaggio fraudolento e una misura sicura da adottare.

03

Per approfondire: quali fasi della catena di un attacco di ingegneria sociale sono più efficaci da bloccare e perché?

5. Fondamenti normativi: GDPR e NIS2 nel settore turistico

La protezione dei dati e la sicurezza digitale nel settore turistico sono disciplinate da due principali quadri normativi: il **GDPR**, che si concentra sulla tutela dei dati personali e dei diritti degli interessati, e la **Direttiva NIS2**, che mira a rafforzare la resilienza dei servizi digitali e la sicurezza della catena di fornitura.

Ai sensi del GDPR, le organizzazioni sono tenute a proteggere i dati personali attraverso misure quali la minimizzazione dei dati, il controllo degli accessi e la tempestiva notifica delle violazioni dei dati personali (data breach). Il Regolamento generale sulla protezione dei dati (**GDPR**)⁶ è applicabile in tutta l'Unione europea dal maggio 2018 e ha introdotto un quadro normativo comune per la tutela dei dati personali e della privacy. Il suo obiettivo è proteggere la riservatezza delle persone e garantire che le organizzazioni siano responsabili delle modalità con cui i dati personali vengono raccolti, conservati e utilizzati.

⁶ Parlamento europeo e Consiglio dell'Unione europea. (2016). *Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)*. Gazzetta ufficiale dell'Unione Europea. <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>

Ad esempio, se la scansione del passaporto di un ospite viene esposta a soggetti non autorizzati, l'organizzazione deve intervenire immediatamente per contenere l'incidente, valutarne il rischio per gli interessati e, ove previsto, notificare l'accaduto all'autorità competente e alle persone coinvolte. Ritardi o interventi incompleti possono aumentare i danni per gli ospiti e comportare conseguenze di natura normativa.

NIS2 e resilienza digitale nella catena di fornitura

La **Direttiva NIS2**⁷ costituisce il quadro normativo dell'Unione europea volto a rafforzare la sicurezza e la resilienza dei servizi e delle reti digitali. Essa impone alle organizzazioni e ai fornitori di servizi essenziali o importanti di gestire i rischi digitali, garantire la continuità dei servizi e segnalare gli incidenti che provocano gravi interruzioni operative o che interessano partner collegati.

Mentre il GDPR si concentra sulla protezione dei dati personali, la **NIS2** riguarda la **resilienza e la continuità dei servizi digitali**. La direttiva richiede alle organizzazioni e ai fornitori di servizi essenziali o importanti di adottare misure efficaci di gestione del rischio digitale e di notificare gli incidenti che compromettono o minacciano la disponibilità dei servizi.

Ad esempio, la compromissione di un gateway di pagamento che impedisce l'elaborazione delle carte di credito in più hotel dimostra perché la resilienza operativa e la segnalazione tempestiva degli incidenti da parte dei fornitori siano essenziali. Quando un singolo fornitore subisce un incidente, l'impatto può propagarsi rapidamente a tutte le organizzazioni connesse.

La NIS2 rafforza inoltre gli obblighi relativi alla gestione del rischio e alla segnalazione degli incidenti lungo tutta la catena di fornitura, coinvolgendo fornitori critici e prestatori di servizi. Poiché le organizzazioni turistiche dipendono fortemente da sistemi esterni, come PMS, CRS e piattaforme di pagamento, controlli inadeguati presso un fornitore possono trasmettere il rischio all'intera filiera. Una conformità insufficiente o notifiche tardive prolungano i tempi necessari per contenere gli incidenti e aumentano la probabilità di un'escalation normativa, con possibili sanzioni più elevate, obblighi di comunicazione pubblica e interruzioni dei servizi che possono coinvolgere partner e clienti.

⁷ Parlamento europeo e Consiglio dell'Unione europea. (2022). *Direttiva (UE) 2022/2555 del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersecurity nell'Unione (Direttiva NIS2)*. Gazzetta ufficiale dell'Unione Europea. <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>

L'**Agenzia dell'Unione Europea per la Cybersicurezza** (ENISA, 2025)⁸ fornisce linee guida tecniche dettagliate sull'attuazione delle misure di gestione del rischio previste dalla Direttiva NIS2. Le indicazioni pongono particolare attenzione alla valutazione strutturata dei rischi, alle procedure di rilevazione e segnalazione degli incidenti, ai controlli di sicurezza lungo la catena di fornitura e ai meccanismi di miglioramento continuo, tutti elementi di fondamentale importanza per gli ecosistemi turistici fortemente interconnessi.

Misure pratiche per ridurre il rischio normativo e operativo

Per ridurre l'esposizione ai rischi e migliorare la conformità normativa, le organizzazioni dovrebbero adottare azioni pratiche e coordinate:

- minimizzare la quantità di dati personali raccolti e conservati;
- definire chiaramente ruoli e responsabilità nei contratti con fornitori e partner;
- applicare controlli sugli accessi e, ove opportuno, utilizzare la crittografia;
- assicurarsi che il personale sappia quando e come segnalare gli incidenti;
- testare le procedure di risposta agli incidenti e di comunicazione insieme ai principali fornitori.

Queste misure consentono di ridurre i tempi di rilevazione e di risposta agli incidenti, limitare l'esposizione a responsabilità legali e mantenere la fiducia dei clienti durante e dopo un incidente.

Per approfondire

Le carenze nella conformità al GDPR, come la notifica tardiva di una violazione dei dati personali, accordi incompleti con i fornitori o una registrazione inadeguata degli incidenti, riducono la possibilità di contenere efficacemente un incidente. Se combinate con sistemi fortemente interconnessi, tali carenze possono consentire alle minacce di propagarsi ai partner, determinare un aggravamento delle misure di vigilanza da parte delle autorità e trasformare una violazione locale dei dati in una crisi che coinvolge più organizzazioni dell'intero ecosistema turistico. Questo dimostra come le mancanze in materia di conformità possano amplificare sia la

⁸ Agenzia dell'Unione Europea per la Cybersicurezza (ENISA). (2025). *Linee guida tecniche per l'attuazione delle misure di gestione del rischio di cibernsicurezza (Versione 1.0)*. https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf

portata sia l'impatto degli incidenti digitali, estendendone gli effetti ben oltre l'organizzazione direttamente interessata.

Riflessione e discussione

01

Descrivi due obblighi del GDPR che il personale deve rispettare e spiega perché sono importanti.

02

Indica tre sistemi che aumentano l'esposizione ai rischi e descrivi come una violazione di uno di essi possa incidere sulle persone e sulle attività aziendali.

03

Per approfondire: in che modo una mancata conformità al GDPR può aggravare un incidente lungo la catena di fornitura digitale?

6. Ruoli, responsabilità e procedure di escalation

La chiara definizione dei ruoli e la tempestiva attivazione delle procedure di escalation sono fondamentali quando si verifica un incidente digitale. Non appena un problema viene individuato, deve essere immediatamente segnalato al referente designato. Questo primo passaggio è essenziale perché una segnalazione tempestiva consente di preservare le prove e di attivare una risposta coordinata, evitando interventi isolati o improvvisati.

Nella maggior parte delle organizzazioni, la gestione di un incidente coinvolge diversi ruoli ben definiti:

- il **segnalatore dell'incidente**, che individua il problema e lo comunica;
- il **primo responsabile dell'intervento** (first responder), generalmente appartenente al reparto IT o alla sicurezza, che verifica l'effettiva presenza dell'incidente;
- il **responsabile della gestione dell'incidente** (incident manager), che coordina le decisioni e le attività di risposta;
- i **team IT o di sicurezza**, che attuano le misure tecniche di contenimento e ripristino;
- il **team di comunicazione**, che gestisce le comunicazioni interne ed esterne verso gli stakeholder;

- **l'ufficio legale o compliance**, che valuta gli obblighi normativi, contrattuali e di notifica.

Ciascun ruolo è responsabile di specifiche attività, garantendo che i rischi tecnici, legali e reputazionali siano affrontati parallelamente e gestiti in modo corretto.

Gli standard internazionali, come la ISO/IEC 27001:2022 ⁹, sottolineano l'importanza di ruoli chiaramente definiti, procedure documentate e una risposta strutturata agli incidenti nell'ambito di un Sistema di Gestione della Sicurezza delle Informazioni (Information Security Management System – ISMS). Questi principi rafforzano la necessità di responsabilità ben definite e di procedure di escalation controllate all'interno delle organizzazioni del settore turistico.

L'importanza della documentazione

Una documentazione accurata in ogni fase della gestione di un incidente è fondamentale. Registrare **cosa è accaduto, quando sono state intraprese le diverse azioni e chi ha autorizzato le decisioni** consente di creare una traccia documentale affidabile (audit trail). Ciò facilita le indagini, gli obblighi di segnalazione alle autorità e le attività di apprendimento successive all'incidente. Una buona documentazione contribuisce inoltre a ridurre i tempi di ripristino, permettendo ai team di identificare le azioni che si sono dimostrate efficaci ed evitare il ripetersi degli stessi errori. Soprattutto, tutela sia il personale sia l'organizzazione nel caso in cui le decisioni adottate vengano successivamente esaminate dalla direzione, dalle autorità di controllo o dai partner.

Perché gli incidenti non dovrebbero essere gestiti individualmente

I dipendenti non dovrebbero mai tentare di risolvere autonomamente un incidente digitale. Interventi individuali possono compromettere le prove forensi, estendere involontariamente la portata dell'incidente o provocare ulteriori perdite di dati. Il personale dovrebbe invece attenersi alle istruzioni del responsabile della gestione dell'incidente (incident manager) o del team IT/sicurezza, consentendo un contenimento controllato dell'incidente e il corretto svolgimento delle procedure di notifica.

⁹ Organizzazione Internazionale per la Normazione. (2022). *ISO/IEC 27001:2022 Sicurezza delle informazioni, cybersecurity e protezione della privacy — Sistemi di gestione della sicurezza delle informazioni — Requisiti*.
<https://www.iso.org/standard/27001>

È importante ricordare che gli incidenti digitali hanno conseguenze concrete sulle persone e sul lavoro quotidiano. I clienti possono subire danni, il carico di lavoro del personale aumenta durante la gestione dell'emergenza e le conseguenze per l'organizzazione diventano più gravi quando l'escalation viene ritardata o gestita in modo inadeguato.

Per approfondire

Modelli semplici di responsabilità, di attribuzione delle responsabilità, come la **matrice RACI**, aiutano a chiarire i ruoli nei momenti di maggiore pressione, definendo con precisione chi deve svolgere ciascuna attività durante un incidente. In una matrice RACI:

- **Responsible (responsabile operativo):** la persona o il team che esegue l'attività;
- **Accountable (responsabile finale):** la persona che ha la responsabilità ultima e approva le decisioni;
- **Consulted (consultato):** le persone che forniscono competenze o consulenza;
- **Informed (informato):** le persone che devono essere aggiornate sull'evoluzione della situazione.

Nel caso della rilevazione di un incidente, il membro del personale che individua e segnala il problema è Responsible, mentre il responsabile della gestione dell'incidente è Accountable. Per il contenimento dell'incidente, i team IT o di sicurezza sono Responsible, mentre l'incident manager mantiene il ruolo di Accountable, coinvolgendo i team di supporto competenti come Consulted e aggiornando gli stakeholder principali come Informed.

Questo approccio strutturato riduce le incertezze, evita la duplicazione delle attività e accelera il processo decisionale durante il limitato tempo disponibile per la risposta agli incidenti.

Riflessione e discussione

01

Perché i dipendenti dovrebbero evitare di cercare di risolvere autonomamente gli incidenti digitali?

02

Indica due motivi per cui la documentazione è importante durante la gestione di un incidente.

03

Per approfondire:

Nell'esempio RACI riportato, chi è responsabile (responsible) del contenimento dell'incidente e chi ne è responsabile finale (accountable)?

Risposta agli incidenti per le piccole imprese del settore turistico

Molte imprese del settore turistico sono realtà di piccole dimensioni, nelle quali il titolare, il responsabile o un numero limitato di dipendenti svolgono contemporaneamente più funzioni. Spesso non sono disponibili team dedicati alla cibersecurity; di conseguenza, le procedure di risposta agli incidenti devono essere semplici, pratiche e facili da applicare.

Un modello di risposta essenziale può aiutare le organizzazioni a reagire rapidamente quando si verifica un incidente informatico:

1. Rilevare	riconoscere attività sospette o comportamenti insoliti
2. Contenere	limitare l'impatto isolando, ove possibile, i dispositivi, gli account o i sistemi interessati
3. Segnalare	informare la persona competente, il supporto IT esterno, il fornitore di servizi o l'autorità competente
4. Ripristinare	ripristinare la normale operatività e individuare gli insegnamenti utili a prevenire incidenti simili in futuro

Anche le piccole organizzazioni possono rispondere efficacemente agli incidenti se il personale sa cosa fare e a chi rivolgersi. Procedure semplici, segnalazioni tempestive e responsabilità chiaramente definite sono spesso più importanti di soluzioni tecniche complesse.

7. La sicurezza digitale nelle attività quotidiane del settore turistico

La sicurezza digitale è realmente efficace **solo quando viene integrata nelle attività operative quotidiane**. I concetti presentati in questa unità, tra cui l'igiene informatica, la consapevolezza dei rischi legati all'ingegneria sociale, la comunicazione sicura e la gestione responsabile dei dati dei clienti, assumono particolare importanza nelle situazioni di lavoro di ogni giorno. Gli incidenti digitali raramente hanno origine da attacchi sofisticati. Più spesso **derivano da piccole scorciatoie operative** adottate durante i periodi di maggiore lavoro, quando il personale è sotto pressione, deve operare rapidamente o gestisce contemporaneamente più richieste. Sebbene possano sembrare insignificanti, queste decisioni quotidiane influenzano direttamente il livello di rischio digitale.

Il rapporto di causa-effetto è semplice:



Una scorciatoia potrebbe non causare danni. Tuttavia, scorciatoie ripetute indeboliscono progressivamente le barriere di protezione. Con il tempo, ciò crea **vulnerabilità strutturali** che i truffatori possono sfruttare.

Come le decisioni quotidiane aumentano il rischio

Tra i comportamenti operativi più comuni che aumentano l'esposizione ai rischi vi sono:

- riutilizzare le credenziali di accesso "solo per oggi";
- rimandare gli aggiornamenti di sistema perché le attività operative sono particolarmente intense;
- condividere gli accessi per velocizzare i processi;
- ignorare messaggi di avviso apparentemente poco importanti;
- rinviare la segnalazione di un incidente.

Singolarmente, queste azioni possono sembrare di scarsa importanza. Ripetute nel tempo, però, riducono la **responsabilità individuale, la tracciabilità delle attività**

e l'integrità dei sistemi. Di conseguenza, aumenta la probabilità di **esposizione dei dati, frodi o interruzioni dei servizi.**

È importante esserne consapevoli: efficienza operativa e sicurezza digitale devono sostenersi a vicenda, non entrare in conflitto.

Tipiche situazioni di “zona grigia”

Le zone grigie sono situazioni in cui il personale deve scegliere tra la rapidità di esecuzione e il rispetto rigoroso delle procedure. Non si tratta di violazioni intenzionali, ma di momenti in cui è necessario esercitare un giudizio.

Esempio 1 – Accesso condiviso durante un periodo di intenso lavoro

Un membro del personale lascia aperta la sessione su un sistema per evitare di effettuare ripetutamente l'autenticazione.

Rischio: accessi non sorvegliati, azioni non autorizzate, uso improprio dei dati.

Esempio 2 – Condivisione temporanea delle credenziali

Le credenziali di accesso vengono condivise per consentire a un collega di iniziare rapidamente il lavoro.

Rischio: perdita della tracciabilità, violazione degli obblighi di conformità, impossibilità di ricostruire gli eventi durante un'indagine.

Esempio 3 – Segnalazione ritardata

Alla fine del turno compare un messaggio insolito del sistema, ma non viene segnalato immediatamente.

Rischio: ritardo nel contenimento dell'incidente e aggravamento dei danni tecnici.

In tutti questi casi, l'obiettivo immediato è la praticità. Nel lungo periodo, però, il risultato può essere una **maggiore esposizione ai rischi** e una **riduzione del controllo.**

Perché piccole deviazioni possono causare incidenti

Quando comportamenti non sicuri vengono ripetuti nel tempo, finiscono per diventare la normalità. Di conseguenza, il personale può smettere di percepirla i rischi.

Esempio di evoluzione del problema:

- "solo questa volta" si condividono le password;
- la condivisione diventa abituale;
- più persone utilizzano lo stesso account;
- non è più possibile attribuire chiaramente le responsabilità;
- indagine difficile dopo una violazione

Gli incidenti digitali si verificano spesso quando più piccole vulnerabilità si manifestano contemporaneamente.

Per questo motivo:

- ruoli chiari sono fondamentali;
- una segnalazione costante e tempestiva è essenziale;
- le buone pratiche di igiene informatica devono diventare un'abitudine.

Una solida sicurezza digitale si costruisce attraverso la disciplina quotidiana, non soltanto grazie agli strumenti tecnologici. La sicurezza digitale dipende dall'interazione tra controlli tecnici e comportamenti responsabili. Quando, nelle attività quotidiane, si trascurano anche piccole regole, l'organizzazione perde gradualmente il controllo su chi può accedere ai dati, modificare le informazioni o individuare tempestivamente i problemi. Ciò riduce la **visibilità**, la **responsabilità individuale** e la **rapidità di risposta**. Con la diminuzione del controllo aumenta la probabilità di **violazioni dei dati**, **perdite economiche**, **conseguenze legali e danni reputazionali**. La disciplina quotidiana protegge quindi sia l'organizzazione sia le persone che dipendono dai suoi sistemi.

Per approfondire

Le piccole scorciatoie operative non aumentano soltanto il rischio tecnico: possono anche rivelare **debolezze nella cultura della gestione del rischio e nei sistemi di controllo**. Quando le decisioni tipiche delle "zone grigie" sono frequenti, ciò può indicare responsabilità poco chiare, una supervisione insufficiente oppure sistemi di valutazione che premiano maggiormente la rapidità rispetto alla sicurezza).

Un'analisi avanzata del rischio si concentra sull'individuazione di:

- dove le scorciatoie si verificano più frequentemente;
- perché il personale si sente spinto a ignorare i controlli;
- quali barriere hanno fallito (tecniche, procedurali o organizzative);
- come più piccole debolezze abbiano contribuito a generare un unico incidente.

Anziché chiedersi "Chi ha commesso l'errore?", la gestione avanzata del rischio si domanda: **"Quale livello di controllo ha fallito e come può essere rafforzato il sistema?"**

Migliorare la resilienza digitale richiede quindi sia:

- misure tecniche di protezione;
- un allineamento organizzativo tra gli obiettivi di efficienza operativa e le aspettative in materia di sicurezza.

Riflessione e discussione

01

Perché piccole scorciatoie operative possono aumentare il rischio digitale nel tempo?

02

Che cos'è una situazione di "zona grigia" nella sicurezza digitale?

03

Perché è importante analizzare i fallimenti dei controlli invece di concentrarsi solo sugli errori individuali?

Risorse video supplementari

Come risorsa introduttiva di approfondimento si propone un video realizzato da **Simplilearn** (2023), che offre una panoramica dei principali concetti di sicurezza informatica e delle diverse tipologie di minacce informatiche.

Canale: Simplilearn

Anno: 2023

Titolo: What Is Cyber Security | How It Works?

YouTube: <https://www.youtube.com/watch?v=inWWhr5tnEA>

8. Verifica delle conoscenze ed esercitazioni

Quiz sulla Consapevolezza della sicurezza digitale

Obiettivo: verificare la comprensione dei principali concetti di cybersicurezza, delle buone pratiche di igiene informatica e degli aspetti normativi fondamentali.

Modalità: Valutazione individuale

Durata stimata: 20–30 minuti

Domande:

1. Perché il settore turistico è considerato ad alto rischio dal punto di vista della sicurezza digitale?
 - A. Perché utilizza più servizi cloud rispetto ad altre settori.
 - B. Perché si basa su un elevato volume di transazioni e su sistemi digitali interconnessi.
 - C. Perché le imprese turistiche non formano il personale in ambito informatico.
 - D. Perché gestisce pochi dati personali.

Risposta corretta: B

2. Quale delle seguenti definizioni descrive meglio una vulnerabilità?
 - A. Un tipo di malware.
 - B. Una debolezza che può essere sfruttata da una minaccia.
 - C. Un requisito normativo.
 - D. Un incidente di sicurezza.

Risposta corretta: B

3. Quali azioni riducono il rischio di compromissione di un account? (Seleziona DUE risposte)
 - A. Abilitare l'autenticazione a più fattori (MFA).

- B. Condividere le password durante l'alta stagione per velocizzare il lavoro.
- C. Usare password robuste e univoche.
- D. Lasciare aperte le sessioni per facilitare il cambio turno.

Risposte corrette: A, C

4. Un membro del personale riceve un'e-mail urgente da un fornitore noto che chiede di modificare immediatamente i dati di pagamento. Qual è il comportamento più sicuro?
- A. Aggiornare immediatamente i dati di pagamento per evitare interruzioni del servizio.
 - B. Inoltrare l'e-mail ai colleghi per avere conferma.
 - C. Verificare la richiesta attraverso un canale indipendente (ad esempio telefonando a un numero già noto).
 - D. Ignorare il messaggio.

Risposta corretta: C

5. Ai sensi del GDPR, le organizzazioni devono (Seleziona TRE risposte):
- A. Proteggere i dati personali mediante adeguate misure di sicurezza.
 - B. Notificare le autorità competenti quando previsto in caso di violazione dei dati.
 - C. Conservare tutti i dati dei clienti senza limiti di tempo.
 - D. Limitare la raccolta dei dati a quelli strettamente necessari.

Risposte corrette: A, B, D

6. Qual è lo scopo principale della Direttiva NIS2?
- A. Eliminare tutti gli incidenti informatici.
 - B. Rafforzare la resilienza dei digitali e la segnalazione degli incidenti.
 - C. Regolamentare i prezzi nel settore turistico.

D. Aumentare l'esternalizzazione dei servizi IT.

Risposta corretta: B

7. Perché l'utilizzo di account condivisi negli ambienti di lavoro del settore turistico rappresenta un rischio?
- A. Perché migliora la velocità operativa.
 - B. Perché riduce la responsabilità individuale e la tracciabilità delle attività.
 - C. Perché rende più semplice l'indagine sugli incidenti.
 - D. Perché facilita gli adempimenti di conformità.

Risposta corretta: B

8. Quale delle seguenti situazioni rappresenta una decisione di "zona grigia"?
- A. Bloccare il computer quando ci si allontana dalla postazione.
 - B. Rifiutarsi di condividere le credenziali di accesso anche sotto pressione.
 - C. Lasciare aperta la sessione di un sistema durante un periodo di intenso lavoro per evitare di autenticarsi ripetutamente.
 - D. Segnalare immediatamente un'attività sospetta.

Risposta corretta: C

9. Perché i dipendenti dovrebbero evitare di gestire autonomamente un incidente digitale? (Seleziona DUE risposte)
- A. Perché potrebbero compromettere le prove o aggravare la violazione.
 - B. Perché dimostrerebbero eccessiva iniziativa.
 - C. Perché garantirebbero una risoluzione più rapida.
 - D. Perché potrebbero non rispettare le procedure interne di escalation.

Risposte corrette: A, D

10. In una matrice RACI relativa al contenimento di un incidente, chi è normalmente l'Accountable?
- A. Il tecnico IT che esegue l'intervento.
 - B. Il responsabile della gestione dell'incidente (Incident Manager) che coordina la risposta.
 - C. Il membro dello staff che ha segnalato il problema.
 - D. Il cliente coinvolto dall'incidente.

Risposta corretta: B

11. Perché piccole scorciatoie operative possono trasformarsi, nel tempo, in veri e propri incidenti?
- A. Perché aumentano la velocità del sistema.
 - B. Perché normalizzano comportamenti non sicuri nel tempo.
 - C. Perché attivano automaticamente gli avvisi di sicurezza.
 - D. Perché eliminano la necessità di segnalare gli incidenti.

Risposta corretta: B

12. Quale comportamento favorisce maggiormente la resilienza digitale nel settore turistico?
- A. Ignorare messaggi di avviso apparentemente poco importanti durante i periodi di maggiore lavoro.
 - B. Segnalare immediatamente attività insolite attraverso i canali previsti.
 - C. Condividere l'accesso ai sistemi con colleghi di fiducia.
 - D. Rimandare gli aggiornamenti alla fine della stagione.

Risposta corretta: B

13. Perché la risposta a una possibile violazione dei dati deve seguire procedure definite e non decisioni informali?

- A. Per evitare di compromettere le prove e garantire il rispetto degli obblighi normativi.
- B. Per ridurre il carico di lavoro della direzione.
- C. Perché la responsabilità è esclusivamente dei fornitori esterni.
- D. Perché gli incidenti digitali si risolvono automaticamente se vengono ignorati.

Risposta corretta: A

Esercitazione 1 – Individuazione dei segnali di allarme del phishing

Obiettivo: rafforzare la capacità di riconoscere tentativi di phishing e di ingegneria sociale nei contesti di comunicazione del settore turistico.

Modalità: discussione di gruppo o analisi plenaria.

Durata stimata: 20–25 minuti.

I partecipanti analizzano un'email sospetta simulata e individuano gli elementi che possono indicare un tentativo di frode.

Da: Booking Support <support@booking-example.com>

A: Reception dell'hotel

Oggetto: URGENTE: Aggiornamento delle coordinate bancarie per i prossimi pagamenti

Gentile Team dell'Hotel,

Vi chiediamo di aggiornare con urgenza il conto bancario per i prossimi pagamenti degli ospiti. In allegato trovate l'ultima fattura.

Il mancato aggiornamento potrebbe causare ritardi nei pagamenti.

Grazie,

Booking Support Team

Allegato: Fattura_0723.pdf

Segnali di allarme da individuare (discussione):

- 🚩 linguaggio che crea urgenza o pressione;
- 🚩 allegato inatteso;
- 🚩 saluto generico ("Gentile Team dell'Hotel ");
- 🚩 dominio del mittente leggermente diverso o sconosciuto.

Esercitazione 2 – Assegnazione delle priorità ai rischi digitali

Obiettivo: sviluppare un approccio strutturato alla valutazione dei rischi digitali nelle attività operative.

Modalità: attività in piccoli gruppi.

Durata stimata: 25–30 minuti.

I partecipanti classificano i comportamenti elencati in base a: a) probabilità che si verifichino; b) impatto potenziale nel caso vengano sfruttati e c) priorità di escalation. Successivamente, ogni gruppo deve fornire una breve motivazione scritta (2–3 frasi) delle proprie scelte, spiegando come probabilità e impatto interagiscono tra loro e perché alcuni comportamenti richiedono una priorità di escalation maggiore.

Comportamenti da classificare in base alla gravità o alla probabilità:

- ❖ Lasciare aperte le sessioni su computer condivisi;
- ❖ Utilizzare password deboli o ripetute;
- ❖ Condividere le credenziali con i colleghi;
- ❖ Cliccare su link provenienti da mittenti sconosciuti;
- ❖ Ignorare gli avvisi di sistema o del software;
- ❖ Rimandare gli aggiornamenti del software;
- ❖ Collegare dispositivi personali ai sistemi aziendali senza autorizzazione;
- ❖ Inoltrare email contenenti informazioni sensibili.

Esercitazione 3 – Applicazione del quadro normativo

Obiettivo: verificare la comprensione dei principali riferimenti normativi e delle loro implicazioni operative.

Modalità: esercizio individuale.

Durata stimata: 5-10 minuti.

Abbina ciascun riferimento normativo al suo obiettivo principale. Successivamente, fornisci un esempio pratico nel settore turistico in cui tale normativa trova applicazione.

Normativa	Obiettivo principale
GDPR	Proteggere i dati personali e garantire il rispetto della normativa sulla privacy
Direttiva NIS2	Rafforzare la resilienza dei servizi digitali e la segnalazione degli incidenti
Data Governance Act	Regolamentare l'utilizzo e la condivisione responsabile dei dati tra organizzazioni
Codice etico globale per il turismo dell'UNWTO	Promuovere pratiche etiche e un turismo sostenibile

Esercitazione 4 – Dibattito strutturato: velocità o sicurezza?

Affermazione da discutere: "Durante l'alta stagione, il personale dovrebbe poter ignorare alcuni passaggi di verifica per mantenere elevata la velocità operativa."

Obiettivo: sviluppare il pensiero critico sul compromesso tra efficienza operativa e sicurezza digitale.

Modalità: Dibattito strutturato (squadre *pro* contro squadra *contro* la affermazione).

Durata stimata: 25-30 minuti.

Le squadre preparano argomentazioni affrontando i seguenti aspetti:

- le pressioni legate all'efficienza operativa;
- l'aumento dei rischi per la sicurezza;
- le implicazioni normative;
- l'impatto sugli ospiti, sul personale e sulla reputazione dell'organizzazione.

Concludere con una riflessione di gruppo su come trovare un equilibrio tra rapidità operativa e sicurezza digitale.

2.2 La sicurezza nei processi digitali del turismo

Al termine di questa sottounità, gli studenti saranno in grado di seguire procedure sicure per prenotazioni e pagamenti, gestire in modo responsabile i dati dei clienti, agire correttamente in caso di sospetta violazione dei dati e collaborare con i team IT e di sicurezza.

- Gestione sicura dei dati dei clienti: protezione delle prenotazioni e dei pagamenti online;
- Blockchain per pagamenti e oltre i pagamenti (tracciamento, verifica dell'identità, programmi fedeltà);
- Protocolli di risposta alle violazioni dei dati (ruoli e responsabilità nelle prime 24 ore).

Attività pratica suggerita:

- Esercitazione basata su uno scenario: attività di pagamento sospetta.

1. Processi digitali nel turismo e punti di rischio

I processi digitali sono ormai integrati in quasi tutte le fasi dell'interazione con gli ospiti. Dal momento della prenotazione fino alla conclusione del soggiorno, i dati dei clienti transitano attraverso molteplici sistemi. Questi processi sono progettati per garantire efficienza e qualità del servizio, ma ogni interazione digitale introduce una potenziale esposizione ai rischi.

Un **punto di rischio digitale** si verifica ogni volta che i dati vengono creati, inseriti, modificati, archiviati, trasmessi o consultati. Quanto più un processo è complesso e interconnesso, tanto più frequentemente i dati vengono trasferiti tra sistemi e utenti. Ogni passaggio aumenta l'esposizione sia a errori accidentali sia a utilizzi impropri intenzionali.

La relazione tra complessità del processo e rischio segue una logica cumulativa:

- più sistemi coinvolti → più punti di integrazione;
- più utenti coinvolti → più credenziali di accesso da gestire;
- più scambi automatizzati → maggiore dipendenza dalle corrette configurazioni dei sistemi;

- più partner esterni coinvolti → maggiore esposizione ai rischi lungo la catena di fornitura (supply chain).

Dove si concentrano più frequentemente i punti di rischio

I punti di rischio nei processi turistici si presentano più spesso nelle seguenti situazioni operative:

1. **Inserimento dei dati e gestione delle prenotazioni:** l'inserimento manuale dei dati nei sistemi PMS o CRS può causare errori, duplicazioni o divulgazioni accidentali di informazioni. Se i controlli di autenticazione sono deboli, persone non autorizzate potrebbero accedere ai dati delle prenotazioni.
2. **Elaborazione dei pagamenti:** le fasi di pagamento rappresentano obiettivi particolarmente sensibili perché coinvolgono dati finanziari. Tra i principali rischi rientrano:
 - connessioni di pagamento non sicure;
 - schemi di transazione insoliti;
 - incongruenze nelle informazioni di fatturazione;
 - ripetuti tentativi di autorizzazione non riusciti;
 - frodi con carta non presente (card-not-present fraud).

Se tali anomalie non vengono riconosciute o segnalate tempestivamente, possono verificarsi perdite economiche e storni di pagamento (chargeback).

3. **Trasferimenti dei dati tra sistemi:** Le integrazioni automatiche tra PMS, CRM, piattaforme di prenotazione e gateway di pagamento migliorano l'efficienza operativa, ma introducono anche rischi legati alle interdipendenze tra sistemi. Configurazioni errate o credenziali compromesse in un sistema possono propagare il problema alle piattaforme collegate.
4. **Gestione degli accessi e cambi di turno:** le modifiche ai permessi degli utenti, l'utilizzo di postazioni condivise e i cambi di turno rappresentano momenti in cui la responsabilità individuale può diminuire. Scorciatoie temporanee possono compromettere la tracciabilità delle attività e rendere più difficile l'indagine in caso di incidente.

Interazione tra rischio tecnico e fattore umano

I punti di rischio operativi derivano dall'interazione tra vulnerabilità tecniche e comportamento umano. Una debolezza tecnica, come una configurazione non sicura, può rimanere latente fino a quando non viene innescata da un errore umano. Allo

stesso tempo, una piccola scorciatoia operativa può esporre una vulnerabilità del sistema che, altrimenti, rimarrebbe innocua.

Ad esempio:

- un addetto alla reception riutilizza le proprie credenziali per velocizzare il check-in;
- un account email compromesso viene utilizzato per reimpostare una password;
- un aggiornamento rimandato lascia irrisolta una vulnerabilità già nota.

Singularmente, queste azioni possono sembrare di scarsa importanza. Combinandosi, però, possono creare le condizioni per incidenti di notevole gravità.

Igiene digitale fisica

I rischi digitali negli ambienti turistici non riguardano esclusivamente il software e i flussi di dati. Molti incidenti hanno origine dall'**accesso fisico ai sistemi digitali**, soprattutto in contesti operativi come le reception degli hotel, le postazioni di lavoro condivise o gli uffici amministrativi.

Dispositivi lasciati incustoditi, controlli insufficienti sugli accessi fisici o l'utilizzo di dispositivi esterni possono creare punti di ingresso per i truffatori. In ambienti particolarmente dinamici, caratterizzati da numerosi cambi di turno e da un continuo contatto con gli ospiti, questi rischi risultano ancora più elevati.

Tra gli esempi più comuni vi sono:

- lasciare incustodito un terminale per il check-in mentre la sessione è ancora aperta;
- consentire l'accesso ad aree amministrative o sale server senza supervisione;
- collegare dispositivi USB sconosciuti a computer aziendali;
- visualizzare informazioni sensibili su schermi facilmente visibili agli ospiti.

Anche azioni apparentemente banali, come lasciare aperta la porta della sala server per favorire la ventilazione, possono compromettere misure di sicurezza digitale altrimenti efficaci.

Per questo motivo, l'igiene digitale fisica dovrebbe essere considerata parte integrante delle attività operative quotidiane, affiancando i controlli tecnici e riducendo la probabilità che piccole disattenzioni si trasformino in incidenti più gravi.

Definizione delle priorità dei rischi nelle attività turistiche

Il rischio digitale negli ambienti turistici non dovrebbe essere valutato in modo intuitivo, ma attraverso un processo strutturato di definizione delle priorità. Due dimensioni principali ne determinano l'urgenza:

- **Probabilità** (likelihood): probabilità che l'evento si verifichi.
- **Impatto** (impact): possibili conseguenze operative, economiche, normative e reputazionali.

Una semplice matrice di valutazione del rischio consente di definire priorità di intervento proporzionate al livello di rischio:

Impatto / Probabilità	Basso	Medio	Alto
Impatto basso	Basso	Basso	Basso
Impatto medio	Basso	Medio	Medio
Impatto alto	Medium	Alto	Critico

I rischi caratterizzati da elevata probabilità ed elevato impatto richiedono un intervento e misure di mitigazione immediate. I rischi a priorità inferiore devono comunque essere monitorati, ma potrebbero non richiedere lo stesso livello di risorse o la medesima urgenza.

Il ruolo del personale nella gestione dei punti di rischio

Il personale svolge un duplice ruolo all'interno dei processi digitali: è sia utilizzatore sia elemento di protezione. Il comportamento dei dipendenti influisce direttamente sulla possibilità che un punto di rischio si trasformi in un incidente.

Il personale dovrebbe:

- seguire le procedure previste durante l'inserimento o la modifica dei dati;
- verificare le richieste insolite prima di intraprendere qualsiasi azione;
- monitorare eventuali schemi di transazione anomali;
- evitare di condividere le credenziali di accesso, anche solo temporaneamente;
- segnalare immediatamente sospette irregolarità attraverso i canali stabiliti.

Come sottolineato nella sottounità 2.1, una segnalazione tempestiva (early escalation) è fondamentale per evitare che irregolarità circoscritte si trasformino in incidenti sistemici. In contesti operativi quali l'elaborazione dei pagamenti e la gestione delle prenotazioni, un ritardo nella segnalazione aumenta significativamente l'esposizione ai rischi finanziari e normativi.

Gli incidenti digitali nei processi turistici hanno conseguenze concrete. Gli ospiti possono subire perdite economiche o violazioni della privacy, mentre le organizzazioni possono andare incontro a danni reputazionali e a obblighi di natura normativa. La continuità operativa dipende quindi da comportamenti responsabili in ogni fase del processo digitale.

Per approfondire

La mappatura dei rischi lungo l'intero percorso digitale del cliente rappresenta un metodo strutturato per analizzare l'esposizione ai rischi. Invece di valutare singole attività in modo isolato, le organizzazioni analizzano:

- dove vengono raccolti i dati;
- dove vengono archiviati;
- dove vengono trasferiti tra sistemi diversi;
- dove cambiano i permessi di accesso;
- dove intervengono fornitori esterni.

Il livello di rischio è generalmente più elevato nei punti di transizione, soprattutto quando i dati cambiano proprietario oppure vengono trasferiti da un sistema a un altro. La mappatura di queste fasi consente alle organizzazioni di concentrare le misure di controllo sui punti a maggiore impatto, anziché distribuire uniformemente le risorse lungo tutte le fasi del processo.

Attività pratica: mappatura dei punti di rischio in un processo turistico reale

Obiettivo: individuare i principali punti di rischio digitale all'interno di un processo tipico del settore turistico.

Modalità: lavoro in piccoli gruppi (3–4 partecipanti)

Durata stimata: 45–60 minuti

In piccoli gruppi, scegliere uno dei processi tipici del settore turistico, ad esempio:

- gestione di una prenotazione online;
- elaborazione di un rimborso;
- gestione di prenotazioni di gruppo;

Unità di Formazione 2: La sicurezza digitale nel turismo

- aggiornamento dei dati degli ospiti durante il check-in;
- coordinamento con una piattaforma di prenotazione esterna.

Per il processo selezionato, identificare:

- un punto di rischio durante l'inserimento dei dati;
- un punto di rischio durante il trasferimento dei dati tra sistemi;
- un rischio legato al comportamento umano;
- un momento in cui potrebbe essere necessario effettuare una segnalazione o attivare la procedura di escalation.

Per ciascun punto di rischio individuato, descrivere brevemente:

- cosa potrebbe andare storto;
- quale potrebbe essere la conseguenza;
- una misura preventiva.

Dopo 10–15 minuti, ciascun gruppo presenta i risultati della propria analisi al resto dei partecipanti.

Riflessione e discussione

01

Che cos'è un punto di rischio digitale e perché i punti di rischio aumentano nei processi digitali?

02

Fornisci un esempio di un rischio durante l'elaborazione dei pagamenti e indica la corretta azione che un dipendente dovrebbe intraprendere.

03

Perché analizzare il rischio lungo l'intero percorso del cliente è più efficace che esaminare ogni fase separatamente?

2. Gestione sicura dei dati dei clienti

La gestione sicura dei dati dei clienti rappresenta una **responsabilità operativa fondamentale** per le organizzazioni del settore turistico. I dati relativi alle prenotazioni, alle informazioni identificative, ai recapiti e ai pagamenti vengono elaborati quotidianamente attraverso sistemi CRM e piattaforme interconnesse. Questi sistemi migliorano l'efficienza del servizio e consentono di offrire esperienze personalizzate, ma concentrano anche grandi quantità di dati personali strutturati. Se i controlli sono insufficienti, possono diventare punti di elevata esposizione ai rischi.

Una protezione efficace dei dati inizia da una raccolta mirata delle informazioni. Le organizzazioni dovrebbero raccogliere esclusivamente i dati necessari per erogare il servizio e adempiere agli obblighi di legge. Raccogliere informazioni aggiuntive solo per comodità aumenta la quantità di dati sensibili conservati e, di conseguenza, l'impatto potenziale in caso di compromissione dei sistemi.

Questo principio, noto come **minimizzazione dei dati**, riduce il rischio in termini pratici:

- minore quantità di dati sensibili archiviati;
- minore impatto in caso di violazione dei dati;
- monitoraggio e controllo più semplici;
- minore esposizione agli obblighi di conformità in caso di incidente.

Limitare la raccolta dati non rappresenta un vincolo tecnico, bensì una decisione strategica di gestione del rischio.

Il principio della minimizzazione dei dati è espressamente previsto dall'articolo 5, paragrafo 1, lettera c), del Regolamento generale sulla protezione dei dati (GDPR), secondo cui i dati personali devono essere "*adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*" (Regolamento (UE) 2016/679).¹⁰

Controllo degli accessi e misure di protezione dei sistemi

¹⁰ Unione europea. (2016). *Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati* (Regolamento generale sulla protezione dei dati – GDPR). Gazzetta ufficiale dell'Unione Europea.
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679>

Dopo la raccolta dei dati, adeguate misure di sicurezza devono garantire che solo il personale autorizzato possa accedere o trattare le informazioni dei clienti.

I principali controlli comprendono:

- **Autorizzazioni di accesso basate sui ruoli**, allineate alle mansioni lavorative (gli accessi vengono assegnati in base al ruolo ricoperto, ad esempio amministrazione o risorse umane, in modo che ciascun utente possa utilizzare solo gli strumenti necessari alle proprie attività).
- **Applicazione del principio del privilegio minimo**, che assegna agli utenti esclusivamente i permessi strettamente necessari allo svolgimento delle proprie mansioni, limitando i danni in caso di compromissione di un account.
- **Autenticazione a più fattori (MFA)**, che richiede due o più elementi di verifica dell'identità (ad esempio password e codice ricevuto sul telefono), rendendo insufficiente il solo furto della password.
- **Crittografia dei dati sensibili**, sia durante l'archiviazione (at rest) sia durante la trasmissione (in transit), in modo che le informazioni risultino illeggibili a soggetti non autorizzati.
- **Registrazione e monitoraggio degli accessi, delle esportazioni e delle modifiche ai dati**, creando una traccia delle operazioni effettuate che consenta di individuare e analizzare rapidamente eventuali attività sospette.

Negli ambienti CRM, il monitoraggio è particolarmente importante. Indicatori quali accessi in orari insoliti, esportazioni ripetute di dati, modifiche massive ai record o accessi da località inattese possono essere segnali di utilizzo improprio o di compromissione dei sistemi. Un'individuazione tempestiva limita significativamente il rischio di escalation.

Una gestione sicura degli accessi richiede inoltre particolare attenzione durante i cambi di personale, i cambi di turno e le modifiche delle mansioni. La mancata revoca tempestiva dei permessi o l'utilizzo di credenziali condivise riducono la tracciabilità delle attività e aumentano l'esposizione ai rischi.

Comportamenti operativi e procedure di escalation

Le misure tecniche, da sole, non sono sufficienti. La gestione sicura dei dati dipende in egual misura da comportamenti responsabili e disciplinati da parte del personale.

Il personale dovrebbe:

- evitare di memorizzare dati relativi ai pagamenti nei campi di testo libero o nelle note interne;
- evitare di esportare dati se non strettamente necessario per motivi operativi;
- seguire le procedure formali previste per la correzione o la cancellazione dei dati;
- disconnettersi dai sistemi quando non sono in uso;
- verificare sempre richieste di accesso insolite o inattese.

Come evidenziato nelle sezioni precedenti, intervenire autonomamente durante un sospetto incidente può compromettere le tracce di audit (audit trail) e rendere più complessa la valutazione richiesta dalla normativa. La segnalazione attraverso i canali previsti garantisce invece la conservazione delle prove e un processo decisionale coordinato.

Una segnalazione tempestiva consente al reparto IT e alla direzione di valutare le misure di contenimento e stabilire se sussistano obblighi di notifica. Un intervento rapido riduce direttamente le interruzioni operative e i danni reputazionali.

Conservazione, cancellazione e integrazione sicura dei dati

La sicurezza dei dati non riguarda soltanto gli accessi e il monitoraggio. Conservare le informazioni più a lungo del necessario aumenta l'esposizione ai rischi senza apportare benefici operativi. Politiche chiare di conservazione e cancellazione dovrebbero definire:

- i periodi di conservazione dei dati relativi a prenotazioni e soggiorni;
- l'anonimizzazione o tokenizzazione delle informazioni relative ai pagamenti;
- le procedure di autorizzazione per la cancellazione dei dati;
- la documentazione delle operazioni di cancellazione.

Anche l'integrazione sicura con le piattaforme di pagamento riveste un ruolo fondamentale. I sistemi CRM dovrebbero evitare di conservare i dati completi delle carte di pagamento, salvo nei casi strettamente necessari e conformi agli standard di sicurezza previsti. Quando possibile, l'utilizzo della tokenizzazione o di gateway di pagamento sicuri riduce la concentrazione del rischio finanziario.

Infine, la verifica periodica delle procedure di risposta agli incidenti, compresa la collaborazione con il reparto IT e con i fornitori esterni, completa il ciclo di gestione sicura dei dati. Le attività di rilevazione, contenimento, documentazione e comunicazione devono operare in modo coordinato.

Nel loro insieme, queste misure costituiscono un quadro strutturato per la protezione dei dati:

raccolta controllata → accesso limitato → uso monitorato → conservazione definita
→ cancellazione documentata.

Attività pratica: Esercitazione di valutazione dei rischi in un sistema CRM

I partecipanti analizzano una struttura CRM semplificata che contiene: recapiti degli ospiti, documenti d'identità scansionati, numero completo della carta di pagamento, note interne, cronologia delle attività di marketing, dati delle prenotazioni archiviati da dieci anni.

1. Identificare quali elementi rappresentano la maggiore esposizione ai rischi.
2. Identificare quali dati potrebbero eccedere le reali necessità operative.
3. Proporre un miglioramento relativo al controllo degli accessi.
4. Proporre un miglioramento della politica di conservazione dei dati.
5. Spiegare quale cambiamento ridurrebbe maggiormente il rischio complessivo e perché.

Per approfondire

Una valutazione avanzata della minimizzazione dei dati prevede un'analisi strutturata dei seguenti aspetti:

- distinzione tra dati obbligatori e dati facoltativi;
- flussi automatici di dati e integrazioni con sistemi esterni;
- tempi di conservazione e verifica dell'effettiva cancellazione;
- utilizzo di tecniche di pseudonimizzazione o tokenizzazione;
- coerenza tra le reali esigenze operative e le informazioni effettivamente conservate.

Concentrare gli interventi correttivi sui dati non necessari che vengono conservati più a lungo consente di ottenere la maggiore riduzione dell'esposizione ai rischi.

Riflessione e discussione

01

Che cos'è la minimizzazione dei dati e perché rappresenta una misura strategica di gestione del rischio?

02

Indica due misure di protezione operative per i dati del CRM e spiega in che modo una di esse riduce l'impatto di un incidente.

03

Per approfondire: Come daresti priorità agli interventi di miglioramento in un sistema CRM che conserva una quantità eccessiva di dati?

3. Pagamenti, frodi e truffe nelle prenotazioni

I pagamenti e le prenotazioni rappresentano fasi ad alto valore nei processi digitali del settore turistico, poiché coinvolgono direttamente transazioni finanziarie e la fiducia dei clienti. A differenza di una generica esposizione dei dati, gli incidenti che riguardano i pagamenti producono spesso conseguenze immediate e misurabili, come perdite economiche, storni di pagamento (chargeback), danni reputazionali e un aumento del carico di lavoro operativo.

Nel settore turistico, le frodi prendono frequentemente di mira i punti in cui avvengono trasferimenti di denaro o in cui esistono obblighi di rimborso. La combinazione di transazioni a distanza, pressione sui tempi e prenotazioni internazionali aumenta ulteriormente la vulnerabilità.

Tipologie più comuni di frode nel settore turistico

Nel settore turistico si riscontrano frequentemente le seguenti tipologie di frode:

- **Frode con carta non presente (Card-not-present – CNP):** utilizzo di dati di carte di pagamento rubati senza che la carta fisica venga verificata;
- **Account rubati o compromessi:** i truffatori ottengono l'accesso ai profili di prenotazione e modificano le prenotazioni esistenti;
- **Truffe nelle prenotazioni con identità false:** prenotazioni fraudolente effettuate per manipolare prezzi o politiche di cancellazione;
- **Business Email Compromise (BEC):** i truffatori si spacciano per fornitori o partner commerciali per indurre l'organizzazione a modificare le coordinate di pagamento;
- **Manipolazione dei rimborsi:** richieste di rimborso fraudolente che sfruttano errori o situazioni di confusione operativa.

I truffatori raramente si affidano esclusivamente a tecniche sofisticate. Molti attacchi sfruttano piuttosto il senso di urgenza, la fiducia o scorciatoie procedurali.

Segnali di allarme e indicatori operativi

Un'efficace individuazione delle frodi si basa sul riconoscimento di **schemi ricorrenti**, più che sull'analisi di singole anomalie. Tra i principali segnali di allarme negli ambienti di pagamento e prenotazione figurano:

- importi di prenotazione insolitamente elevati;
- numerose prenotazioni effettuate in rapida successione dallo stesso account o indirizzo IP;
- incongruenze tra dati di fatturazione e informazioni di contatto;
- ripetuti tentativi di autorizzazione non riusciti;
- richieste urgenti di modifica delle coordinate di pagamento;
- pressioni per ignorare le normali procedure di verifica.

Considerati singolarmente, questi segnali possono indicare semplici irregolarità operative e non necessariamente una frode. Tuttavia, il loro valore aumenta notevolmente quando vengono analizzati nel loro insieme.

Per facilitare una valutazione strutturata, gli indicatori di frode possono essere suddivisi in tre livelli:

- **Anomalie isolate:** una singola transazione anomala o un'incongruenza senza altri elementi ricorrenti.
- **Anomalie ricorrenti:** irregolarità ripetute dallo stesso indirizzo IP, dispositivo, account o metodo di pagamento.
- **Indicatori di frode coordinata:** combinazione di più segnali, come numerose prenotazioni effettuate in rapida successione, incongruenze nell'identità e messaggi che fanno leva sull'urgenza.

Gli indicatori appartenenti al livello più elevato richiedono una segnalazione immediata (escalation), poiché spesso indicano attività fraudolente organizzate e non semplici errori operativi. Dare priorità ai segnali combinati migliora l'efficacia dell'individuazione delle frodi e riduce inutili interruzioni delle attività.

Risposta operativa a transazioni sospette

Quando un pagamento o una prenotazione appaiono sospetti, è necessario seguire procedure strutturate, evitando decisioni improvvisate.

Il personale dovrebbe:

- Sospendere temporaneamente l'elaborazione della transazione;
- evitare di effettuare rimborsi o modifiche senza un'adeguata verifica;
- richiedere una conferma aggiuntiva attraverso i canali autorizzati;
- coinvolgere il reparto amministrativo, il reparto IT o la direzione secondo le procedure previste;
- documentare tutte le azioni intraprese.

Cercare di "risolvere rapidamente il problema" sotto pressione può aumentare l'esposizione ai rischi. Una procedura di escalation ben definita tutela sia i clienti sia l'organizzazione.

Misure di prevenzione

La prevenzione delle frodi richiede una combinazione di misure tecniche e comportamenti responsabili.

Tra i principali controlli rientrano:

- **Gateway di pagamento sicuri**, che garantiscono l'elaborazione cifrata delle transazioni e riducono l'esposizione dei dati delle carte nei sistemi interni;
- **Autenticazione 3-D Secure (3DS)**, che aggiunge un ulteriore livello di verifica dell'identità del titolare della carta durante i pagamenti online;
- **Monitoraggio delle transazioni e regole di rilevazione automatica**, capaci di individuare schemi insoliti, come prenotazioni ripetute in rapida successione, transazioni improvvisamente di elevato importo o ripetuti tentativi di autorizzazione falliti;
- **Separazione dei compiti nell'approvazione dei pagamenti**, individuare schemi insoliti, come prenotazioni ripetute in rapida successione, transazioni improvvisamente di elevato importo o ripetuti tentativi di autorizzazione falliti;
- **Soglie di escalation definite**, che stabiliscono quando una transazione deve essere esaminata dalla direzione o dal reparto IT anziché essere elaborata automaticamente;
- **Formazione periodica sulla prevenzione delle frodi**, per rafforzare la capacità del personale di riconoscere tecniche di pressione, tentativi di impersonificazione e anomalie nelle prenotazioni.

Nessuna misura è sufficiente da sola. L'adozione di controlli multilivello riduce sia la probabilità sia l'impatto delle frodi.

Contesto normativo

La prevenzione delle frodi nell'elaborazione dei pagamenti è rafforzata dai requisiti normativi europei. **La Direttiva (UE) 2015/2366 relativa ai servizi di pagamento (PSD2)** ¹¹ ha introdotto l'obbligo della Strong Customer Authentication (Autenticazione Forte del Cliente – SCA) per i pagamenti elettronici. La SCA richiede almeno due fattori di autenticazione indipendenti ed è comunemente implementata tramite meccanismi come 3-D Secure (3DS).

Per le organizzazioni del settore turistico, ciò significa che la verifica sicura dei pagamenti non rappresenta soltanto una buona pratica, ma costituisce parte di un quadro normativo finalizzato a ridurre le frodi online e a tutelare i consumatori nell'Unione Europea.

Scenario

L'incidente:

Un'e-mail proveniente da un fornitore storico comunica che il proprio conto bancario è cambiato e richiede l'aggiornamento urgente delle coordinate di pagamento. Il messaggio sottolinea che il mancato aggiornamento immediato potrebbe causare l'interruzione del servizio in occasione di un evento imminente.

"Se non aggiornate subito questi dati, non potremo consegnare il cibo per il banchetto di matrimonio di questa sera!"

Attività di gruppo

1. Individuare i segnali di allarme presenti nel messaggio.
2. Quali rischi comporterebbe elaborare la richiesta senza effettuare verifiche?
3. Quali procedure di verifica dovrebbero essere seguite?
4. Quali procedure di escalation dovrebbero essere attivate?
5. Quale misura di controllo avrebbe potuto prevenire o limitare il rischio?

Per approfondire

¹¹ Unione europea. (2015). *Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno (PSD2)*. Gazzetta ufficiale dell'Unione Europea.
<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366>

L'analisi dei modelli di frode consiste nell'individuare gli indicatori che meglio consentono di riconoscere attacchi organizzati o automatizzati. Prenotazioni effettuate in rapida successione, transazioni improvvisamente di importo elevato, ripetuti tentativi di autorizzazione falliti e incongruenze relative all'indirizzo IP o al dispositivo utilizzato rappresentano spesso segnali di attività fraudolente strutturate.

Concentrare il monitoraggio su questi indicatori ad alto impatto migliora l'efficacia dell'individuazione delle frodi e riduce inutili rallentamenti delle attività operative.

Riflessione e discussione

01

Indica due tipologie comuni di frode nei pagamenti nel settore turistico e un indicatore per ciascuna.

02

Qual è la corretta risposta immediata quando una transazione appare sospetta?

03

Perché la pressione operativa può aumentare il rischio di frode?

04

Per approfondire:
Quali indicatori di frode dovrebbero avere la priorità nei sistemi di monitoraggio e perché

4. Esercitazione basata su uno scenario: pagamento sospetto

Attività pratica

Obiettivo: applicare la gerarchia individuazione delle frodi e le procedure strutturate di escalation.

Modalità: analisi di uno scenario in piccoli gruppi

Durata stimata: 30–40 minuti

Descrizione dello scenario:

Un membro dell'ufficio amministrativo riceve un'e-mail da un fornitore storico (ad esempio un servizio di lavanderia o un distributore alimentare). La richiesta appare plausibile: il rapporto con il fornitore è reale e il momento coincide con un pagamento programmato.

Il messaggio riporta:

"Gentile Ufficio Amministrazione, in allegato trova le nuove coordinate bancarie per la prossima fattura mensile. Il nostro precedente conto corrente è in fase di chiusura a causa di un audit. La preghiamo di aggiornare immediatamente i vostri dati e di confermare quando sarà effettuato il pagamento previsto per la prossima settimana. Il mancato aggiornamento potrebbe comportare la sospensione del servizio."

Allegato: [Nuove_Coordinate_Bancarie_e_Fattura.pdf](#)

Discussione di gruppo: come reagire?

Gli studenti analizzano lo scenario in piccoli gruppi concentrandosi su tre fasi di valutazione strutturata: individuazione del punto di rischio, riconoscimento dei segnali di allarme e definizione della corretta risposta operativa.

Fase 1: Individuazione del punto di rischio

Discutere:

- Perché l'ufficio amministrativo rappresenta un obiettivo ad alto valore?
- Quali responsabilità operative rendono questo reparto particolarmente vulnerabile?

Elemento chiave da considerare:

L'ufficio amministrativo dispone dell'autorità necessaria per modificare le coordinate di pagamento ed effettuare trasferimenti di denaro. Una compromissione in questa fase può causare perdite economiche immediate, anziché conseguenze indirette o differite nel tempo.

Fase 2: Riconoscimento dei segnali di allarme

Individuare i possibili segnali di allarme, come:

- linguaggio che trasmette urgenza e pressione;
- richiesta di modificare coordinate bancarie già consolidate;
- minaccia di sospensione del servizio;
- spiegazione inaspettata relativa alla chiusura del conto corrente;
- allegato che richiede un'azione immediata.

Anche in assenza di link dannosi, il rischio deriva dalla manipolazione delle procedure operative e non necessariamente dalla presenza di malware.

Questo scenario rappresenta un esempio tipico di **Business Email Compromise** (Compromissione di email aziendali – BEC).

Fase 3: Definizione di una risposta strutturata

Gli studenti determinano la corretta sequenza di azioni.

Le risposte appropriate includono:

- sospendere temporaneamente la modifica delle coordinate di pagamento;
- evitare di aggiornare immediatamente i dati bancari;
- verificare la richiesta attraverso un canale indipendente (ad esempio telefonando al fornitore utilizzando un numero già noto e verificato);
- effettuare la segnalazione interna seguendo le procedure di controllo finanziario previste;
- documentare tutte le azioni intraprese.

La verifica deve essere effettuata attraverso un canale di comunicazione separato. Utilizzare i recapiti presenti nell'e-mail sospetta non costituisce una verifica indipendente.

Gli studenti dovrebbero anche riflettere su:

- in quale momento sia opportuno coinvolgere la direzione o il reparto IT;
- in che modo la documentazione delle attività protegga sia il dipendente sia l'organizzazione;
- quale misura di controllo già esistente (ad esempio la separazione dei compiti) avrebbe potuto prevenire o limitare questo scenario.

5. Le prime 24 ore dopo una violazione dei dati

Quando viene rilevata una **violazione dei dati**, le prime 24 ore sono decisive. Le decisioni prese in questa fase influenzano l'entità dell'impatto, l'esposizione ai rischi

normativi, le interruzioni operative e i danni reputazionali. Ritardi o interventi non coordinati possono aumentare significativamente le conseguenze dell'incidente.

La priorità immediata è **il contenimento**. Contenere una violazione significa isolare i sistemi interessati, interrompere gli accessi non autorizzati e impedire che l'incidente si estenda ulteriormente. Se il contenimento viene ritardato, possono essere esposti ulteriori dati, il ripristino dei sistemi diventa più complesso e aumentano i costi economici e reputazionali.

Il contenimento, tuttavia, deve essere effettuato in modo controllato e accuratamente documentato.

Priorità immediate nelle prime 24 ore

La risposta iniziale dovrebbe concentrarsi sulle seguenti azioni: identificare i sistemi coinvolti e le categorie di dati interessate; isolare gli account o i sistemi compromessi; conservare i registri di sistema (log) e le prove disponibili; informare i referenti previsti dalle procedure di escalation interne; documentare tutte le azioni intraprese. La conservazione delle prove è particolarmente importante. Tentativi non coordinati di "ripulire" i sistemi possono eliminare elementi utili alle analisi forensi, rendendo più difficile l'indagine e aumentando il rischio di non conformità agli obblighi normativi.

Come già evidenziato, interventi non coordinati possono involontariamente ampliare la portata della violazione o compromettere le prove necessarie all'indagine. Nelle prime 24 ore sono quindi essenziali una procedura di escalation disciplinata e un contenimento controllato, per limitare l'esposizione ai rischi normativi e reputazionali.

Documentazione e audit trail

Una documentazione accurata durante le prime 24 ore è fondamentale. È opportuno predisporre una cronologia chiara degli eventi che registri:

- **quando** è stata rilevata la violazione;
- **che** l'ha segnalata;
- **quali sistemi** sono stati coinvolti;
- **quali azioni di contenimento sono state adottate;**
- **chi** ha autorizzato le decisioni.

Questo audit trail supporta le attività di indagine, le comunicazioni alle autorità competenti e l'analisi dell'incidente a fini di miglioramento. Inoltre, tutela il personale dimostrando che le procedure previste sono state correttamente seguite.

LE PRIME 24 ORE DOPO UNA VIOLAZIONE DEI DATI

Azioni critiche per limitare l'impatto, proteggere le persone e garantire la conformità normativa

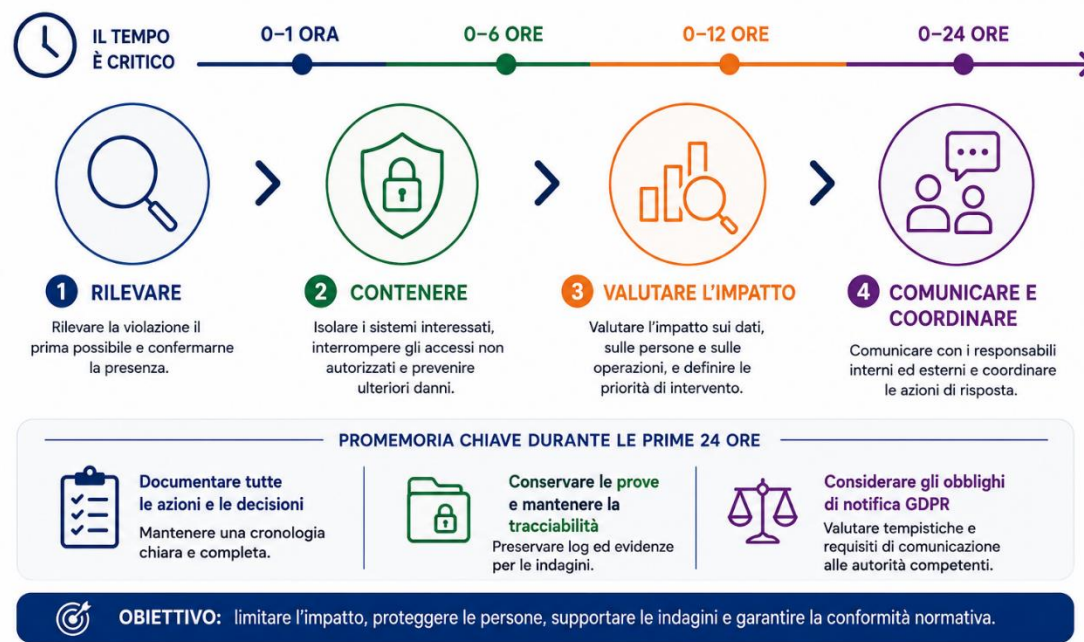


Figura 3: Fasi chiave di risposta durante le prime 24 ore dopo una violazione dei dati

Aspetti normativi

Ai sensi dell'articolo 33(1) del Regolamento Generale sulla Protezione dei Dati (GDPR, 2016), le organizzazioni devono notificare la violazione dei dati personali all'autorità di controllo competente entro 72 ore dal momento in cui ne vengono a conoscenza, salvo che sia improbabile che la violazione comporti un rischio per i diritti e le libertà delle persone fisiche.

"In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza (...), a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche." (GDPR, 2016, Art. 33)

Inoltre, l'**articolo 34** prevede che l'organizzazione comunichi direttamente la violazione **alle persone interessate** quando essa possa comportare un rischio elevato per i loro diritti e le loro libertà.

Ciò significa che, nelle prime 24 ore, l'organizzazione non deve limitarsi a contenere la violazione, ma deve anche effettuare una **valutazione preliminare strutturata dell'impatto**, al fine di determinarne le conseguenze operative e normative. In particolare, è necessario valutare:

- se sono coinvolti dati personali;
- il livello di rischio per le persone interessate;
- se sia necessario notificare l'autorità di controllo competente;
- se sia opportuno informare direttamente le persone coinvolte.

Una valutazione tempestiva e strutturata consente di ridurre sia l'esposizione ai rischi normativi sia i danni reputazionali.

Per supportare questa valutazione, le organizzazioni dovrebbero applicare un **modello rapido di valutazione dell'impatto**, basato su criteri predefiniti:

1. sensibilità dei dati coinvolti (ad esempio dati identificativi, dati di pagamento, dati sanitari o informazioni sugli spostamenti);
2. numero di registrazioni potenzialmente interessate dalla violazione;
3. criticità dei sistemi coinvolti (sistemi essenziali per l'operatività oppure sistemi di supporto);
4. potenziale esposizione a rischi normativi.

L'utilizzo di una semplice scala di valutazione da 1 a 3 per ciascun criterio consente di stabilire priorità motivate, adottare misure di contenimento proporzionate e supportare le decisioni relative alla notifica dell'autorità di controllo entro il termine di 72 ore previsto dal GDPR.

Comunicazione e reputazione

Durante la prima giornata, l'organizzazione dovrebbe predisporre un **piano di comunicazione sia interno sia esterno**. La comunicazione deve essere accurata, basata sui fatti e coordinata tra tutte le funzioni coinvolte. Dichiarazioni premature o speculative possono aumentare la confusione e aggravare i danni reputazionali.

Gli incidenti digitali influenzano i clienti, aumentano il carico di lavoro del personale e possono compromettere la stabilità dell'organizzazione. Essere consapevoli di questi effetti rafforza l'importanza di un intervento tempestivo e strutturato.

Scenario: mappatura della risposta nelle prime 24 ore

Un membro del personale segnala che, durante la notte, un utente non autorizzato ha avuto accesso al sistema di prenotazione. Diversi dati relativi agli ospiti potrebbero essere stati consultati o esportati.

In piccoli gruppi, gli studenti dovranno:

- definire le prime tre azioni da intraprendere;
- individuare quali figure professionali devono essere informate;
- stabilire se possa essere necessaria una notifica alle autorità competenti;
- individuare quali informazioni devono essere documentate nelle prime 24 ore

Ogni gruppo dovrà motivare le proprie decisioni sulla base dell'impatto e del livello di rischio.

Per approfondire

Reagire rapidamente è fondamentale, ma intervenire senza un approccio strutturato può aumentare l'esposizione ai rischi. Azioni affrettate possono portare a trascurare obblighi normativi o a compromettere prove utili alle indagini. Al contrario, un'eccessiva prudenza può consentire alla violazione di estendersi ulteriormente.

Una risposta efficace richiede un equilibrio tra rapidità e rispetto delle procedure. Procedure di escalation chiaramente definite, ruoli prestabiliti e decisioni adeguatamente documentate consentono alle organizzazioni di intervenire con tempestività, garantendo al tempo stesso il rispetto dei requisiti normativi e delle esigenze operative.

Riflessione e discussione

01

Qual è la priorità principale nelle prime 24 ore successive a una violazione dei dati e perché?

02

Perché i dipendenti devono segnalare immediatamente gli incidenti invece di cercare di risolverli autonomamente?

03

Quali informazioni devono essere documentate durante la fase iniziale di risposta?

6. Cooperazione con il reparto IT e i fornitori esterni

Una cooperazione efficace il reparto IT e con i fornitori esterni è fondamentale negli ambienti turistici fortemente digitalizzati. Sistemi di prenotazione, pagamenti, CRM, servizi cloud e piattaforme di prenotazione sono spesso gestiti attraverso soluzioni fornite da terze parti. Quando si verifica un incidente, la sua gestione raramente dipende da un solo reparto.

Nel settore turistico, il rischio digitale si estende spesso oltre i confini dell'organizzazione. Vulnerabilità nei sistemi dei fornitori, integrazioni configurate in modo errato o ritardi nella comunicazione possono amplificare l'impatto dell'incidente sull'intero ecosistema digitale.

Collaborazione interna

Quando viene rilevato un problema di sicurezza digitale, è essenziale una collaborazione strutturata tra il personale operativo e il reparto IT.

Il personale operativo è spesso il primo a individuare anomalie, ma il contenimento tecnico richiede competenze specialistiche. Una collaborazione efficace si basa su una comunicazione chiara e su una segnalazione accurata.

Nel segnalare un incidente, il personale dovrebbe fornire:

- data e ora della rilevazione;
- sistema coinvolto;
- account utente interessato;
- descrizione del comportamento anomalo osservato;
- azioni già intraprese.

U Segnalazioni incomplete o poco precise ritardano il contenimento dell'incidente e rendono più difficile l'attività di indagine.

Una chiara definizione dei ruoli evita confusione. Lo personale operativo segnala l'incidente e preserva le informazioni disponibili; il reparto IT analizza l'incidente e isola i sistemi coinvolti; la direzione coordina le decisioni; i responsabili della conformità o l'ufficio legale valutano gli obblighi previsti dalla normativa.

Interventi non coordinati da parte di personale non tecnico possono ampliare involontariamente la portata dell'incidente o compromettere prove utili alle indagini.

Collaborazione con i fornitori esterni

Molte organizzazioni turistiche si affidano a fornitori esterni per sistemi PMS basati su cloud, Online Travel Agencies (OTA), gateway di pagamento, piattaforme CRM e servizi IT in outsourcing. Se un incidente coinvolge sistemi ospitati da fornitori esterni, è fondamentale informarli tempestivamente. Essi potrebbero dover:

- isolare i server interessati;
- disabilitare gli account compromessi;
- fornire i registri di sistema;
- confermare l'effettiva portata della violazione;
- supportare le attività di notifica previste dalla normativa.

Ritardare la comunicazione ai fornitori può prolungare l'esposizione al rischio e aumentare i tempi di inattività dei sistemi.

Accordi contrattuali chiari dovrebbero definire:

- le responsabilità in materia di sicurezza;
- i tempi previsti per la segnalazione degli incidenti;
- i diritti di accesso ai sistemi;
- gli obblighi relativi alla protezione dei dati;
- i diritti di audit e i meccanismi di verifica.

La gestione dei fornitori rappresenta quindi una misura preventiva e non una semplice formalità contrattuale.

Rischio nella catena di fornitura e contesto normativo

Nell'ambito della direttiva NIS2 e delle correlate linee guida europee sulla cybersicurezza, le organizzazioni devono gestire i rischi non solo all'interno dei propri sistemi, ma anche lungo l'intera catena di fornitura.

Le imprese turistiche che si affidano a fornitori digitali interconnessi dovrebbero valutare:

- quali fornitori trattano dati personali;
- quali fornitori dispongono di accesso diretto ai sistemi;
- quali misure di sicurezza sono previste contrattualmente;
- come vengono comunicati e gestiti gli incidenti attraverso le procedure di escalation.

Un incidente che coinvolge un fornitore esterno può rapidamente trasformarsi in un problema che interessa più organizzazioni. Una gestione proattiva dei fornitori contribuisce a ridurre il rischio sistemico.

Documentazione e miglioramento continuo

La collaborazione deve essere documentata in ogni fase della gestione dell'incidente. Le registrazioni delle comunicazioni con il reparto IT e con i fornitori esterni supportano:

- la conformità agli obblighi normativi;
- la revisione dell'incidente;
- l'individuazione di debolezze procedurali;
- la riduzione dei rischi futuri.

La valutazione successiva all'incidente dovrebbe comprendere anche un'analisi dell'efficacia della comunicazione e della rapidità della risposta. La resilienza digitale dipende dalla capacità di coordinarsi efficacemente, non dall'azione dei singoli individui.

Riflessione e discussione

01

Perché è essenziale fornire una segnalazione accurata al reparto IT durante un incidente digitale?

02

Quali informazioni deve fornire il personale operativo quando segnala un incidente?

03

Perché una corretta gestione dei fornitori riduce il rischio sistemico?

7. Tecnologie avanzate per la sicurezza digitale nel turismo

Gli ambienti digitali del settore turistico fanno sempre più affidamento su tecnologie avanzate per **rafforzare la protezione dei dati, la verifica dell'identità e l'integrità delle transazioni**. Sebbene il rispetto delle procedure operative rimanga fondamentale, alcune soluzioni tecnologiche possono ridurre significativamente il rischio sistemico se implementate correttamente.

Le tecnologie di sicurezza avanzate non sostituiscono comportamenti responsabili. Al contrario, rafforzano i controlli esistenti e riducono la probabilità che vulnerabilità umane o tecniche si trasformino in incidenti gravi.

Blockchain e integrità dei dati

La blockchain è una tecnologia di registro distribuito (distributed ledger) progettata per migliorare l'integrità dei dati e la tracciabilità negli ambienti digitali che coinvolgono più soggetti. Collegando le transazioni in una struttura sequenziale resistente alle manomissioni, aumenta la trasparenza e la responsabilità tra sistemi interconnessi.

Negli ecosistemi turistici che coinvolgono diversi attori, come hotel, Online Travel Agencies (OTA) e fornitori di servizi di pagamento, la blockchain può supportare:

- la verifica dell'integrità dei dati di prenotazioni;
- la registrazione delle transazioni in modo resistente alle manomissioni;
- il rafforzamento della fiducia nelle relazioni con i fornitori.

Analisi di settore, come quella di Mize (2023) ¹², suggeriscono inoltre che la blockchain può ridurre le inefficienze nei processi di riconciliazione e aumentare la trasparenza delle transazioni nelle reti di distribuzione turistica.

Il principale contributo della blockchain riguarda la protezione dell'integrità dei dati negli ambienti digitali condivisi. Tuttavia, questa tecnologia non risolve vulnerabilità di tipo comportamentale, come il phishing, l'uso improprio delle credenziali o controlli di accesso insufficienti. La sua efficacia dipende quindi da una governance adeguata, da una gestione strutturata degli accessi e da un'implementazione proporzionata alle reali esigenze operative, piuttosto che dall'adozione di tecnologie per semplice effetto delle tendenze del mercato.

Identità digitale sicura e autenticazione forte

La gestione dell'identità rappresenta uno dei principali punti di controllo nella sicurezza digitale del settore turistico. Credenziali rubate o utilizzate impropriamente costituiscono frequentemente il punto di ingresso per frodi e violazioni dei dati.

¹²Ref. Mize. (2023). *Unlocking the Potential of Blockchain Technology in Travel*.
<https://mize.tech/blog/unlocking-the-potential-of-blockchain-technology-in-travel/>

I sistemi di gestione sicura dell'identità possono includere:

- autenticazione a più fattori (MFA);
- soluzioni di identità federata;
- sistemi di Single Sign-On (SSO) con controlli di accesso condizionati;
- verifica biometrica per le transazioni ad alto rischio.

Una solida verifica dell'identità riduce il rischio di compromissione degli account (account takeover) e limita la propagazione di un attaccante tra sistemi interconnessi. Essa supporta inoltre il principio dello Zero Trust, già introdotto in precedenza: nessuna fiducia implicita e verifica continua di utenti e dispositivi.

Negli ecosistemi in cui interagiscono hotel, OTA e fornitori di servizi di pagamento, un'elevata affidabilità dell'identità digitale contribuisce a ridurre significativamente i rischi tra piattaforme diverse.

Interconnessione dei sistemi e sicurezza dell'ecosistema digitale

Le tecnologie avanzate sono particolarmente rilevanti in ambienti in cui interagiscono numerosi sistemi digitali. Le piattaforme turistiche coinvolgono spesso:

- sistemi di gestione delle strutture ricettive (PMS);
- agenzie di viaggio online (OTA);
- gestori dei pagamenti;
- piattaforme di marketing;
- fornitori di servizi cloud.

Misure tecnologiche quali controlli di sicurezza sulle API, standard di cifratura e sistemi automatici di monitoraggio rafforzano la fiducia tra sistemi interconnessi. Tuttavia, una maggiore complessità tecnologica può introdurre nuove dipendenze. Configurazioni errate o una supervisione insufficiente possono compromettere i benefici attesi.

Valutazione costi-benefici e approccio basato sul rischio

L'adozione di tecnologie avanzate per la sicurezza dovrebbe essere il risultato di una valutazione attenta e non una semplice reazione a un incidente o alle tendenze del mercato. L'introduzione di tali tecnologie richiede infatti risorse economiche, integrazione con i sistemi esistenti, formazione del personale, adeguamento delle procedure operative quotidiane. In molti casi è inoltre necessario rivedere ruoli,

responsabilità e modelli di governance affinché i nuovi controlli funzionino efficacemente all'interno dei processi esistenti.

Una valutazione costi-benefici dovrebbe considerare sia gli effetti immediati sia quelli di lungo periodo, tra cui la riduzione delle perdite dovute alle frodi e delle interruzioni operative, il miglioramento della conformità normativa, e il rafforzamento della fiducia dei clienti. L'obiettivo non è aumentare la complessità tecnologica, ma ottenere un miglioramento proporzionato e dimostrabile della resilienza della sicurezza.

Non tutte le soluzioni sono adatte a ogni organizzazione. Le realtà di dimensioni ridotte possono ottenere un elevato livello di protezione rafforzando i controlli sull'identità digitale e i sistemi di pagamento sicuri, mentre le organizzazioni più grandi e maggiormente interconnesse possono giustificare l'adozione di tecnologie più avanzate quando l'integrità dei sistemi e l'interoperabilità rappresentano esigenze strategiche.

La definizione delle priorità sulla base del rischio consente di mantenere gli investimenti in sicurezza coerenti con il livello di esposizione dell'organizzazione, la dipendenza dai sistemi digitali e il profilo di rischio complessivo.

Il fattore umano rimane centrale

Anche le tecnologie più avanzate non possono compensare pratiche scorrette nella gestione delle password, la mancata segnalazione delle anomalie, l'uso improprio delle credenziali o le scorciatoie procedurali adottate sotto pressione operativa. Questi comportamenti rappresentano spesso il punto di ingresso degli incidenti, indipendentemente dal livello di sofisticazione delle misure tecniche adottate.

La tecnologia rafforza la resilienza organizzativa solo quando è accompagnata da comportamenti operativi disciplinati e responsabili. Sistemi sicuri richiedono utenti responsabili. Controlli sull'identità, strumenti di monitoraggio e meccanismi di cifratura riducono l'esposizione ai rischi, ma non eliminano la necessità di vigilanza e del rispetto delle procedure.

La sicurezza digitale nel turismo è quindi una questione sia tecnologica sia organizzativa. Una resilienza sostenibile dipende dall'interazione tra controlli tecnologici strutturati e comportamenti coerenti e responsabili da parte di tutte le figure coinvolte nelle attività operative.

Questo principio si applica anche al **crescente utilizzo degli strumenti di Intelligenza Artificiale (IA) nel settore turistico**. Sebbene l'IA possa supportare la creazione di contenuti, la comunicazione con i clienti, il marketing e numerose attività operative, il suo impiego deve avvenire **in modo responsabile**, evitando ad esempio di inserire dati personali o informazioni sensibili dei clienti in sistemi di IA pubblici e **rispettando le politiche dell'organizzazione, i requisiti in materia di protezione dei dati e la normativa vigente**.

Il personale dovrebbe inoltre verificare sempre i contenuti generati dall'IA, utilizzare, ove disponibili, servizi di IA approvati dall'organizzazione e garantire che il giudizio umano rimanga centrale nei processi decisionali.

Per approfondire

Gli studenti analizzano come le tecnologie avanzate per la sicurezza si integrino con strategie più ampie, tra cui i principi dello Zero Trust, la resilienza della catena di fornitura prevista dalla direttiva NIS2, la costruzione della fiducia digitale nel lungo periodo e la necessità di soluzioni scalabili negli ecosistemi turistici interconnessi.

Valutano inoltre quale approccio tecnologico possa rafforzare in modo più efficace la resilienza dell'intero ecosistema digitale, anziché limitarsi alla protezione dei singoli sistemi.

Riflessione e discussione

01

Qual è il principale vantaggio della tecnologia blockchain dal punto di vista della sicurezza?

02

Perché la gestione dell'identità è fondamentale per ridurre il rischio digitale?

03

Perché gli investimenti nelle tecnologie di sicurezza devono essere basati sul rischio e non sulle tendenze del mercato?

04

Per approfondire:
Quale controllo avanzato migliorerebbe maggiormente la resilienza sistemica in un contesto con più partner?

8. Riflessione e consolidamento

Riflessione individuale

Ogni studente prepara brevi risposte scritte alle seguenti domande:

1. Quale fase del processo digitale nella tua organizzazione presenta il rischio digitale più elevato e perché?
2. Quale comportamento umano rappresenta la maggiore vulnerabilità?
3. Quale singolo miglioramento ridurrebbe maggiormente il rischio nel tuo ambiente di lavoro?

Le risposte dovrebbero dimostrare la comprensione delle dimensioni operative, comportamentali e normative del rischio digitale.

Analisi in piccoli gruppi

In gruppi di tre o quattro persone, gli studenti confrontano le loro riflessioni e identificano:

- un processo ad alto rischio comune;
- una vulnerabilità comportamentale condivisa;
- un miglioramento concretamente realizzabile.

Ogni gruppo prepara una breve sintesi motivando le proprie conclusioni. L'analisi dovrebbe essere strutturata considerando:

- l'impatto operativo, economico e reputazionale;
- la probabilità che l'evento si verifichi;
- le possibili implicazioni normative.

Successivamente, ogni gruppo presenta sinteticamente le proprie conclusioni, motivando le priorità individuate.

Scenario: escalation durante un fine settimana di alta stagione

È l'inizio della stagione turistica di punta. L'hotel è al completo grazie a una grande conferenza internazionale che si svolge in città.

L'ufficio amministrativo riceve un'e-mail urgente da un fornitore storico che richiede l'immediata modifica delle coordinate bancarie. Il messaggio fa riferimento a un "problema legato a un audit" e avverte che, in assenza dell'aggiornamento, le consegne previste per l'evento potrebbero subire ritardi.

A causa della pressione operativa e della ridotta disponibilità di personale, la modifica viene effettuata senza ulteriori verifiche.

Due giorni dopo, il reparto IT rileva attività di accesso insolite nel sistema CRM. Diversi dati degli ospiti risultano essere stati consultati al di fuori del normale orario di lavoro e non è chiaro se siano stati anche esportati.

Nel frattempo, il fornitore contatta l'organizzazione chiedendo perché il pagamento non sia ancora stato ricevuto. Contemporaneamente, il personale della reception segnala le lamentele di alcuni ospiti che hanno ricevuto sospette e-mail relative a rimborsi.

Con il manifestarsi contemporaneo di più anomalie, la direzione richiede un chiarimento urgente e una valutazione immediata del potenziale impatto.

L'organizzazione si trova ora ad affrontare una possibile combinazione di frode nei pagamenti e violazione dei dati nel pieno della stagione turistica.

Attività di gruppo

In piccoli gruppi, gli studenti analizzano la situazione e delineano:

1. Quale dovrebbe essere la prima azione immediata?
2. Quali figure interne devono essere coinvolte?
3. Quali sistemi devono essere verificati o isolati?
4. Quali informazioni devono essere documentate nelle prime 24 ore?
5. Questa situazione potrebbe comportare un obbligo di notifica ai sensi del GDPR?
6. Quale misura controllo introdotta in precedenza (procedura, comportamento o tecnologia) avrebbe potuto evitare l'escalation?

Ogni gruppo dovrà motivare le proprie decisioni considerando l'impatto operativo, l'esposizione economica, il rischio normativo e le conseguenze reputazionali.

Riflessione finale

Gli studenti dovrebbero riflettere su come la pressione operativa abbia influenzato il processo decisionale e su come piccole deviazioni dalle procedure abbiano contribuito a trasformare un problema iniziale in un incidente più grave. Particolare attenzione dovrebbe essere dedicata all'importanza della verifica tempestiva, delle procedure di escalation strutturate e della collaborazione coordinata con il reparto IT e i fornitori.

Unità di Formazione 2: La sicurezza digitale nel turismo

La discussione dovrebbe evidenziare come procedure rigorose e ben definite proteggano sia il personale sia l'organizzazione, soprattutto durante i periodi di maggiore pressione operativa.



2.3 Simulazioni e gestione delle crisi digitali

Al termine di questa sottounità, gli studenti saranno in grado di reagire correttamente alle emergenze digitali, comunicare in modo chiaro e responsabile, evitare l'escalation dei danni e supportare le azioni di ripristino.

- Tipologie di incidenti informatici: phishing e frodi nelle prenotazioni, ransomware, attacchi DdoS, violazioni dei dati, compromissione degli account;
- Gerarchia della comunicazione: personale interno, clienti, autorità competente (Garante per la protezione dei dati), media;
- Gestione della fase post-incidente: ripristino dei sistemi e ricostruzione della fiducia;
- Pressione psicologica durante una crisi digitale

Attività pratiche suggerite:

- Caso di studio 1: attacco ransomware a un PMS di un hotel.
- Caso di studio 2: campagna di phishing ai danni di una piattaforma di prenotazione.
- Workshop: elaborazione di un piano di comunicazione per crisi da fuga di dati.

1. Tipologie di incidenti digitali nel settore turistico

Gli incidenti digitali si verificano quando i sistemi che gestiscono **prenotazioni, pagamenti o dati dei clienti** subiscono interruzioni, utilizzi impropri o compromissioni. La maggior parte degli incidenti segue una chiara relazione di causa-effetto: una vulnerabilità o un errore umano consente un accesso non autorizzato, un'interruzione del servizio o una manipolazione dei dati, generando successivamente conseguenze operative, economiche, legali o reputazionali.

Riconoscere le diverse tipologie di incidente consente al personale di rispondere in modo proporzionato, evitando reazioni impulsive.

Le principali tipologie di incidenti comprendono:

- **Violazioni dei dati (data breach):** esposizione non autorizzata di dati personali o di pagamento, con possibili obblighi di notifica alle autorità e danni reputazionali.

- **Interruzioni dei sistemi:** indisponibilità di piattaforme essenziali a causa di guasti tecnici o attacchi informatici, con conseguenti interruzioni del servizio e perdite economiche.
- **Incidenti nei pagamenti:** transazioni fraudolente, addebiti errati o storni di pagamento (chargeback) che compromettono la stabilità finanziaria.
- **Accessi non autorizzati:** accesso a sistemi o dati senza le necessarie autorizzazioni, con aumento del rischio di manipolazione o diffusione delle informazioni.
- **Manipolazione della reputazione o campagne di disinformazione:** diffusione coordinata di informazioni false o fuorvianti che compromette la fiducia dei clienti e influenza il comportamento nelle prenotazioni.

Ogni tipologia di incidente produce effetti differenti sui vari soggetti coinvolti. I clienti possono subire perdite economiche o violazioni della privacy; il personale deve affrontare pressioni operative e obblighi di segnalazione; la direzione è chiamata a gestire gli aspetti normativi e i danni reputazionali.

Una risposta efficace inizia con una segnalazione tempestiva, procedure di escalation ben definite e una comunicazione controllata.

Per approfondire

Classificare gli incidenti in base alla loro **gravità** e all'**ampiezza dell'impatto** consente di stabilire priorità proporzionate. Gli incidenti di minore gravità possono essere gestiti a livello locale, mentre quelli che coinvolgono dati sensibili, provocano interruzioni sistemiche o comportano rischi normativi richiedono un'immediata escalation, il coinvolgimento della direzione e una gestione coordinata della crisi.

La gravità di un incidente, tuttavia, non deve essere considerata statica. Negli ambienti digitali del settore turistico gli incidenti evolvono spesso attraverso fasi di escalation ben riconoscibili:

1. **Rilevamento di un'anomalia:** viene osservato un comportamento insolito o un'irregolarità nel sistema;
2. **Compromissione locale:** un sistema, un account o un dispositivo risulta compromesso;
3. **Propagazione laterale:** l'incidente si estende ad altri sistemi interconnessi o ad altri account utente;
4. **Interruzione operativa:** si verificano interruzioni del servizio, perdite economiche o problemi nelle prenotazioni;

- 5. Escalation normativa e reputazionale:** vengono coinvolte le autorità di controllo, si rende necessaria la comunicazione ai clienti e l'incidente assume rilevanza pubblica.

Riconoscere tempestivamente queste fasi di escalation consente di intervenire prima che l'incidente si diffonda, limitando l'impatto operativo e reputazionale e supportando decisioni motivate sotto il profilo normativo. Individuare il problema già nella fase di anomalia o di compromissione locale riduce significativamente i danni per l'organizzazione.

Riflessione e discussione

01

Indica due tipologie di incidenti digitali e una possibile conseguenza per ciascuna.

02

Perché una segnalazione strutturata è essenziale durante un incidente?

03

Per approfondire: In che modo la classificazione della gravità degli incidenti migliora il processo decisionale?

2. Pressione psicologica durante le crisi digitali

Le crisi digitali raramente si verificano in condizioni di tranquillità. Stress, incertezza e pressione temporale riducono l'attenzione e aumentano la probabilità di adottare scorciatoie procedurali. Il sovraccarico cognitivo può indurre il personale a saltare passaggi di verifica o ad agire prematuramente, ampliando potenzialmente l'impatto dell'incidente.

Le ricerche nel campo dei fattori umani e della cybersicurezza dimostrano costantemente che stress, sovraccarico cognitivo e pressione temporale aumentano significativamente la probabilità di errori procedurali durante la risposta agli incidenti, evidenziando l'importanza di procedure di escalation strutturate e di ruoli chiaramente definiti¹³.

Come illustrato nelle sottounità 2.1 e 2.2, la mancata attivazione tempestiva delle procedure di escalation rappresenta spesso un fattore determinante nell'aggravarsi

¹³ Agenzia dell'Unione europea per la cybersicurezza (ENISA). (2019). *Linee guida sulla cultura della cybersicurezza: aspetti comportamentali della cybersicurezza*.
<https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity>

delle crisi. Sotto pressione psicologica, i tentativi individuali di risolvere autonomamente il problema possono compromettere una risposta coordinata e aumentare l'impatto dell'incidente nel lungo periodo.

Procedure ben strutturate contribuiscono a ridurre questi rischi. Percorsi di escalation chiari, responsabilità definite e brevi checklist decisionali limitano le ambiguità. La presenza di un responsabile della gestione dell'incidente (Incident Manager) consente inoltre di centralizzare il coordinamento e di evitare azioni contraddittorie.

Tra le principali misure di stabilizzazione rientrano:

- procedure di pausa e verifica (pause-and-verify) prima di intraprendere azioni irreversibili;
- procedure di segnalazione esercitate regolarmente;
- un supporto visibile da parte della direzione, che incoraggi una tempestiva escalation;
- riunioni di debriefing post-incidente per favorire l'apprendimento e il miglioramento continuo.

La resilienza durante una crisi dipende tanto dalla disciplina nei comportamenti quanto dalle capacità tecniche.

Per approfondire

I responsabili dovrebbero definire soglie decisionali che stabiliscano quando l'attivazione immediata delle procedure di escalation è obbligatoria. Strumenti di supporto alle decisioni, come modelli RACI semplificati o matrici di escalation, favoriscono decisioni coerenti anche in condizioni di stress. Una leadership efficace è in grado di bilanciare rapidità d'intervento, conservazione delle prove e tutela del benessere del personale.

Riflessione e discussione

01

Indica due fattori psicologici che aumentano il rischio di errore durante una crisi.

02

Perché, nelle situazioni di forte pressione, è preferibile seguire la procedura di escalation piuttosto che cercare di risolvere il problema individualmente?

03

Per approfondire: In che modo la leadership può strutturare il processo decisionale per garantire al tempo stesso rapidità e accuratezza?

3. Caso studio 1 – Attacco ransomware al PMS di un hotel

Attività pratica

Obiettivo: dimostrare una risposta coordinata agli incidenti a un incidente in condizioni di pressione operativa.

Modalità: simulazione di gruppo con ruoli assegnati

Durata stimata: 60–90 minuti

Questa attività consente ai partecipanti di applicare i principi della gestione delle crisi in uno scenario simulato di attacco ransomware. I partecipanti si esercitano nell'attivazione delle procedure di escalation, nel processo decisionale coordinato, nella valutazione degli aspetti normativi e nella gestione della comunicazione in condizioni di elevata pressione operativa.

Un hotel di medie dimensioni situato in una città subisce un attacco ransomware durante la notte. All'arrivo del turno mattutino, il personale non riesce ad accedere al Property Management System. I dati delle prenotazioni risultano cifrati, i pagamenti automatici sono bloccati e non è possibile verificare le preautorizzazioni delle carte di pagamento. Nel giro di pochi minuti iniziano a formarsi lunghe code alla reception per il check-in.

Le prime verifiche rivelano che l'attacco è stato avviato da un'e-mail di phishing aperta durante il turno notturno. Il malware è stato eseguito su una postazione di lavoro collegata alla rete del PMS. A causa di una segmentazione della rete insufficiente, il codice malevolo si è propagato lateralmente fino ai sistemi di backup condivisi, rendendoli temporaneamente inutilizzabili.

L'impatto operativo è immediato e in rapido peggioramento. Il personale della reception torna alle procedure di registrazione manuale. Gli ospiti manifestano crescente insoddisfazione per i ritardi. Il reparto amministrativo non è in grado di verificare le transazioni e la direzione deve decidere se interrompere completamente gli accessi ai sistemi esterni, con il rischio di aggravare ulteriormente l'interruzione delle attività.

Nel giro di poche ore, l'hotel si trova ad affrontare molteplici rischi interconnessi. Le operazioni di prenotazione risultano paralizzate, compromettendo check-in e nuove prenotazioni. Le perdite economiche iniziano ad accumularsi a causa delle cancellazioni e degli storni di pagamento (chargeback). Allo stesso tempo, qualora l'integrità dei dati personali fosse stata compromessa, potrebbero sorgere obblighi di notifica previsti dalla normativa. Anche il danno reputazionale aumenta rapidamente,

poiché gli ospiti iniziano a condividere online l'esperienza negativa, amplificando l'impatto ben oltre il guasto operativo iniziale.

Il contenimento dell'incidente richiede il rapido isolamento dei sistemi infetti, la limitazione dell'accesso alla rete, il coinvolgimento di specialisti forensi esterni e la verifica dell'integrità dei backup prima del ripristino. Il completo recupero richiede diverse settimane e comporta un intenso coordinamento tra attività tecniche, operative e di comunicazione.

Valutazione iniziale della situazione

Gli studenti lavorano in piccoli gruppi e devono:

- identificare i rischi operativi, finanziari, normativi e reputazionali immediati;
- stabilire se l'incidente possa configurare una potenziale violazione dei dati personali;
- definire la prima azione operativa da intraprendere entro i primi 30 minuti.

Ogni gruppo presenta una breve motivazione delle proprie decisioni, basata sull'analisi dell'impatto e sulla logica di escalation.

Coordinamento della crisi basato sui ruoli

Agli studenti vengono assegnati specifici ruoli organizzativi:

- Responsabile operativo;
- Responsabile IT;
- Responsabile finanziario;
- Responsabile della comunicazione;
- Responsabile della conformità / Responsabile della protezione dei dati

Ogni gruppo deve concordare su:

- le misure immediate di contenimento;
- le decisioni relative all'isolamento dei sistemi;
- l'eventuale necessità di coinvolgere specialisti forensi esterni;
- l'opportunità di avviare una valutazione del rischio normativo;
- le priorità della comunicazione interna.

Ciascun ruolo illustra brevemente le proprie principali preoccupazioni e priorità decisionali. L'obiettivo è dimostrare una risposta coordinata, anziché interventi isolati.

Escalation sotto pressione mediatica

Il formatore introduce ulteriori sviluppi nello scenario:

- i media riportano la notizia di un "guasto ai sistemi dell'hotel".
- un ospite pubblica online un messaggio chiedendo se i dati della propria carta di pagamento siano stati compromessi.

I gruppi devono decidere:

- quali informazioni possono essere comunicate immediatamente;
- quali aspetti devono rimanere oggetto di verifica;
- chi debba ricoprire il ruolo di portavoce;
- se avviare le procedure di notifica verso soggetti esterni.

Le decisioni devono bilanciare trasparenza, obblighi legali ed esigenze delle indagini forensi.

Analisi delle cause e strategia di prevenzione

I gruppi svolgono una breve revisione strutturata rispondendo alle seguenti domande:

- Quale vulnerabilità ha permesso all'incidente di aggravarsi?
- Quale misura tecnica ridurrebbe maggiormente il rischio che l'evento si ripeta?
- Quale miglioramento comportamentale o procedurale è necessario?
- Quale elemento legato ai fornitori o alla governance ha contribuito all'esposizione al rischio?

Successivamente, i gruppi definiscono un ordine di priorità per le azioni correttive, sulla base della loro efficacia nella riduzione del rischio sistemico.

Per approfondire

Un'analisi strutturata delle cause individua tre principali debolezze sistemiche: il successo dell'attacco di phishing, un'inadeguata segmentazione della rete e la

presenza di backup archiviati nello stesso ambiente accessibile ai sistemi compromessi. Le principali priorità di intervento includono:

- rafforzare i filtri per la posta elettronica e svolgere regolari attività di sensibilizzazione e simulazioni di phishing;
- migliorare la segmentazione della rete per impedire la propagazione laterale del malware;
- implementare backup offline o immutabili;
- rafforzare le procedure di escalation per garantire un rilevamento e una segnalazione più tempestivi degli incidenti.

L'applicazione di un metodo strutturato di revisione (cronologia dell'incidente → analisi delle cause → piano di intervento prioritario) consente di trasformare le lezioni apprese in miglioramenti concreti e misurabili della resilienza organizzativa, anziché in semplici soluzioni temporanee.

4. Caso studio 2 – Campagna di phishing attraverso una piattaforma di prenotazione

Attività pratica

Obiettivo: analizzare come un'impresa turistica dovrebbe rispondere quando gli ospiti diventano bersaglio di una campagna di phishing.

Modalità: discussione di gruppo ed esercizio di problem solving

Durata stimata: 45–60 minuti

Questa attività consente ai partecipanti di analizzare un incidente di phishing che colpisce gli ospiti attraverso una piattaforma di prenotazione ritenuta affidabile. I partecipanti si esercitano nella valutazione dei rischi, nella comunicazione con i clienti, nel coordinamento con partner esterni e nella pianificazione della risposta all'incidente.

Un piccolo hotel inizia a ricevere telefonate da ospiti che hanno ricevuto messaggi in cui viene richiesto un pagamento aggiuntivo per confermare la prenotazione. I messaggi sembrano provenire da una nota piattaforma di prenotazione e contengono un collegamento a una pagina di pagamento.

Diversi ospiti seguono le istruzioni e inseriscono i dati della propria carta di pagamento prima di rendersi conto che i messaggi sono fraudolenti.

L'hotel contatta la piattaforma di prenotazione e scopre che gli attaccanti potrebbero aver ottenuto l'accesso a uno degli account della piattaforma utilizzati per comunicare con gli ospiti. Con l'aumentare delle segnalazioni, gli ospiti iniziano a pubblicare avvisi sui social media e sui siti di recensioni. Il personale dell'hotel non sa quante informazioni possa condividere né come rispondere ai clienti preoccupati.

Valutazione iniziale

Lavorando in piccoli gruppi, discutere i seguenti aspetti:

- Quali sono i principali rischi per gli ospiti?
- Quali sono i principali rischi per l'hotel?
- Quali informazioni sono già disponibili?
- Quali ulteriori informazioni sono necessarie prima di poter prendere decisioni?
- Quali azioni dovrebbero essere intraprese nelle prime ore dopo l'identificazione dell'incidente?

Gestione della situazione

Ogni gruppo rappresenta il team di direzione dell'hotel.

Dovrà discutere e concordare su:

- come informare gli ospiti dell'incidente;
- quali indicazioni fornire agli ospiti coinvolti;
- chi debba comunicare con la piattaforma di prenotazione;
- se sia opportuno pubblicare una comunicazione ufficiale;
- quali azioni possono contribuire a mantenere la fiducia dei clienti.

Alla fine dovrà preparare un breve piano d'azione e spiegare le motivazioni delle decisioni prese.

Revisione e prevenzione

Dopo aver discusso lo scenario, il gruppo rifletterà sulle seguenti domande:

- Perché gli ospiti erano propensi a fidarsi di questi messaggi?
- Quali segnali avrebbero potuto indicare che i messaggi erano fraudolenti?
- Quali misure potrebbero contribuire a prevenire incidenti simili in futuro?
- In che modo le imprese turistiche possono aiutare gli ospiti a riconoscere i tentativi di phishing?

Per approfondire

Questo caso dimostra che gli incidenti informatici non hanno sempre origine nei sistemi dell'organizzazione. Le imprese turistiche dipendono spesso da piattaforme di prenotazione, fornitori di servizi di pagamento e altri partner digitali. Quando uno degli elementi di questo ecosistema viene compromesso, i clienti possono comunque associare il problema alla struttura ricettiva.

Tra le misure che possono ridurre il rischio vi sono:

- attivare l'autenticazione a più fattori per gli account delle piattaforme;
- verificare regolarmente le attività degli account;
- fornire al personale una formazione sul riconoscimento dei tentativi di phishing;
- informare gli ospiti sulle procedure ufficiali di pagamento;
- definire procedure di comunicazione chiare per la gestione degli incidenti digitali.

Questo scenario evidenzia l'importanza della comunicazione con i clienti, della sicurezza delle piattaforme di terze parti e del mantenimento della fiducia durante un incidente digitale.

5. Comunicazione di crisi

Perché la comunicazione determina l'esito di una crisi

Durante un incidente digitale, la comunicazione non rappresenta un'attività secondaria rispetto alla risposta tecnica, ma costituisce un elemento centrale della gestione della crisi. Il modo in cui le informazioni vengono condivise influenza la rapidità del contenimento, la conformità normativa, la fiducia degli stakeholder e la reputazione dell'organizzazione nel lungo periodo. Messaggi poco strutturati o informali possono trasformare rapidamente un incidente tecnico in una crisi reputazionale di più ampia portata.

Quando la comunicazione non è coordinata, aumenta la confusione interna. Il personale può ricevere istruzioni incoerenti, duplicare le azioni o rilasciare dichiarazioni premature agli ospiti o ai media. Tutto ciò non solo rallenta il contenimento dell'incidente, ma può anche aumentare l'esposizione legale e compromettere la fiducia del pubblico. Per questo motivo, la comunicazione di crisi deve essere disciplinata, proporzionata e coordinata strategicamente.

Principi fondamentali della comunicazione

Una comunicazione efficace durante una crisi nel settore turistico si basa su cinque principi:

1. **Accuratezza prima della rapidità:** verificare i fatti prima di comunicare pubblicamente.
2. **Un'unica autorità di riferimento:** designare un portavoce.
3. **Allineamento interno prima della comunicazione esterna:** assicurarsi che il personale comprenda la situazione prima di diffondere messaggi all'esterno.
4. **Trasparenza senza speculazioni:** comunicare ciò che è noto evitando supposizioni.
5. **Tracciabilità della comunicazione:** conservare una documentazione delle comunicazioni per eventuali verifiche legali e normative.

Struttura della comunicazione interna

Subito dopo l'identificazione di un incidente, i team interessati dovrebbero ricevere un breve aggiornamento basato sui fatti. Tale comunicazione dovrebbe chiarire **ciò che è stato confermato, ciò che è ancora oggetto di verifica, le azioni immediate richieste, chi è autorizzato a comunicare con l'esterno.**

Una comunicazione interna chiara riduce l'incertezza e previene iniziative non autorizzate. In situazioni di forte pressione, il personale potrebbe sentirsi spinto a risolvere autonomamente i problemi o a rispondere informalmente alle domande degli ospiti. Un coordinamento interno strutturato limita questi rischi e tutela sia il personale sia la credibilità dell'organizzazione.

Comunicazione verso gli ospiti

La comunicazione con gli ospiti deve bilanciare chiarezza, empatia e precisione delle informazioni. I messaggi dovrebbero spiegare l'impatto operativo dell'incidente, descrivere le **misure immediate adottate** e fornire indicazioni pratiche o canali di assistenza. Il tono deve rimanere calmo e responsabile, evitando atteggiamenti difensivi o conclusioni premature.

Dichiarazioni speculative possono generare ulteriori rischi legali e reputazionali, soprattutto quando non è ancora stato confermato se l'integrità dei dati personali sia stata compromessa. È quindi fondamentale garantire coerenza tra tutti i canali di

comunicazione. Aggiornamenti contraddittori provenienti da reparti diversi possono compromettere seriamente la fiducia dei clienti.

Accessibilità digitale nella comunicazione di crisi

Le strategie di comunicazione di crisi devono **garantire che le informazioni raggiungano tutti gli ospiti**, comprese le persone con disabilità visive, uditive o cognitive. Durante un incidente digitale, affidarsi a un solo canale di comunicazione può escludere alcuni gruppi di utenti, soprattutto se determinati sistemi risultano indisponibili.

Una comunicazione accessibile richiede l'utilizzo di più modalità complementari, ad esempio:

- segnaletica chiara presso la reception o nelle aree comuni;
- spiegazioni verbali o assistenza diretta da parte del personale;
- annunci audio, ove opportuno;
- comunicazioni scritte in linguaggio semplice e comprensibile.

Ad esempio, se i display digitali o le notifiche su dispositivi mobili non sono disponibili, la segnaletica cartacea o la comunicazione diretta del personale possono diventare il principale mezzo di informazione. Garantire l'accessibilità durante una crisi non è soltanto una questione di qualità del servizio, ma anche di sicurezza, inclusione e responsabilità legale.

Comunicazione e conformità normativa

Negli incidenti che possono coinvolgere dati personali, la comunicazione è strettamente collegata agli obblighi previsti dalla normativa. Nell'ambito del GDPR (articoli 33 e 34), la **notifica alle autorità di controllo** e, ove necessario, agli interessati deve essere basata su una valutazione strutturata e non su reazioni emotive. La comunicazione pubblica dovrebbe quindi essere coordinata con il supporto legale, così da garantire la conformità normativa senza compromettere le attività investigative.

Una comunicazione trasparente dimostra responsabilità e affidabilità; tuttavia, una divulgazione prematura potrebbe compromettere le prove forensi o aumentare la responsabilità dell'organizzazione. Trovare il giusto equilibrio tra trasparenza e controllo rappresenta uno dei principali compiti della leadership nella gestione delle crisi.

Attività pratica – Simulazione di comunicazione

Obiettivo: elaborare comunicazioni interne ed esterne strutturate durante un incidente digitale.

Modalità: attività di scrittura in piccoli gruppi

Durata stimata: 45 minuti

I partecipanti lavorano in piccoli gruppi e preparano tre brevi comunicazioni relative a un incidente simulato:

1. Un breve aggiornamento interno (massimo 150 parole);
2. Un comunicato preliminare rivolto agli ospiti;
3. Una risposta a una richiesta di informazioni da parte dei media.

Ogni gruppo dovrà motivare quali informazioni sono state escluse, quali informazioni sono state volutamente omesse, in che modo gli aspetti normativi hanno influenzato la formulazione del messaggio. L'attenzione è rivolta non solo al contenuto delle comunicazioni, ma anche al processo decisionale e al principio di proporzionalità.

Per approfondire: la comunicazione di crisi come processo strutturato

Una gestione avanzata delle crisi riconosce che la comunicazione evolve attraverso fasi distinte, anziché limitarsi a una singola reazione. Negli incidenti digitali, la comunicazione segue generalmente quattro fasi: **preparazione, risposta immediata, stabilizzazione e ricostruzione della fiducia.**

La fase di preparazione comprende la definizione preventiva di ruoli, modelli di comunicazione e procedure di escalation. La risposta immediata si concentra sull'allineamento interno e sulla gestione controllata della comunicazione esterna. La fase di stabilizzazione richiede aggiornamenti coerenti e il coordinamento con gli adempimenti normativi. Infine, la ricostruzione della fiducia va oltre il semplice ripristino tecnico e punta a dimostrare concretamente le misure correttive adottate e l'impegno dell'organizzazione nel lungo periodo.

Considerare la comunicazione come un processo ciclico aiuta le organizzazioni a evitare reazioni impulsive e a mantenere un controllo strategico durante le crisi digitali.

Riflessione e discussione

01

Quale dovrebbe essere il primo passo della comunicazione interna quando viene rilevato un incidente e perché?

02

Perché la comunicazione con gli ospiti deve evitare speculazioni e mantenere coerenza?

6. Recupero post-incidente e ricostruzione della fiducia

Dopo un incidente digitale, il recupero deve essere **rapido** ma anche **strutturato**. Le decisioni prese nelle fasi iniziali determinano se l'interruzione delle attività verrà contenuta efficacemente o se evolverà in una situazione di instabilità prolungata. La priorità iniziale consiste nella stabilizzazione tecnica: **isolare i sistemi compromessi, ripristinare backup verificati e sicuri e mettere in sicurezza i punti di accesso per prevenire nuovi incidenti**.

Tuttavia, il recupero non si limita alla sola riparazione tecnica. La sua gestione deve seguire i principi di risposta strutturata illustrati nelle sezioni precedenti. Azioni correttive frammentarie o non documentate compromettono la resilienza a lungo termine e possono esporre l'organizzazione a ulteriori verifiche da parte delle autorità competenti. Un **recupero efficace** combina quindi il ripristino tecnico con una documentazione accurata, la valutazione degli obblighi normativi e una comunicazione trasparente.

Le principali misure di recupero comprendono:

- verificare l'integrità dei backup prima del ripristino;
- applicare misure di sicurezza compensative a breve termine per ridurre il rischio residuo;
- svolgere un'analisi forense mirata per confermare l'estensione e l'impatto dell'incidente;
- documentare tutte le azioni intraprese ai fini della conformità normativa e degli audit.

Una volta stabilizzati i sistemi, l'attenzione si sposta sulla ricostruzione della fiducia. Questo richiede azioni coerenti e credibili, non semplici rassicurazioni. Le organizzazioni dovrebbero **comunicare chiaramente le misure correttive** adottate, dimostrare i miglioramenti apportati alla sicurezza, ad esempio attraverso

controlli di accesso più efficaci o una migliore segmentazione della rete, e mettere a disposizione **canali di contatto facilmente accessibili per gli stakeholder** coinvolti.

Anche il **supporto al personale** è fondamentale durante la fase di recupero. Fatica e pressione operativa aumentano infatti il rischio di errori successivi. Una pianificazione strutturata delle attività, una chiara assegnazione delle responsabilità e percorsi formativi successivi all'incidente contribuiscono a rafforzare la resilienza organizzativa e dimostrano un approccio responsabile alla gestione della crisi.

Un recupero sostenibile integra il ripristino tecnico, il rafforzamento della governance e la ricostruzione della fiducia. Se gestita correttamente, questa fase rappresenta un'opportunità per aumentare la resilienza dell'organizzazione nel lungo periodo, anziché limitarsi a ripristinare la situazione precedente.

Per approfondire

Una pianificazione avanzata del recupero va oltre la semplice stabilizzazione immediata. La ricostruzione della fiducia nel lungo periodo può comprendere verifiche indipendenti, come audit o certificazioni di terze parti, aggiornamenti periodici e trasparenti destinati a clienti e partner, il rafforzamento dei meccanismi di controllo e garanzia nei confronti dei fornitori, investimenti nel monitoraggio continuo e in un'architettura dei backup più resiliente, inclusi backup immutabili.

Queste misure consentono di trasformare il recupero da una semplice risposta reattiva a un processo di miglioramento strutturale. Gli investimenti successivi all'incidente dovrebbero essere proporzionati alle dimensioni dell'organizzazione e al suo livello di esposizione al rischio, bilanciando i costi con una riduzione misurabile dei rischi futuri e della vulnerabilità reputazionale.

Riflessione e discussione

01

Individua tre priorità immediate durante la fase di ripristino. Spiega perché queste azioni devono essere affrontate prima di avviare gli interventi di miglioramento a lungo termine.

02

Perché una documentazione strutturata delle azioni di ripristino è essenziale? Considera il suo ruolo nella conformità normativa, nell'apprendimento interno, nella responsabilità organizzativa e nella fiducia degli stakeholder.

03

Quali misure a lungo termine sono più efficaci per ricostruire la fiducia digitale in un'organizzazione turistica? Valuta se gli aggiornamenti tecnici, le misure di trasparenza, gli audit indipendenti, le garanzie offerte dai fornitori o la formazione del personale producano il maggiore impatto nel lungo periodo e motiva la tua risposta.

Prospettiva conclusiva: la sicurezza digitale come governance

La sicurezza digitale nel turismo non deve essere considerata una funzione esclusivamente tecnica, ma una disciplina di governance integrata che combina vigilanza operativa, consapevolezza normativa, prioritizzazione strutturata dei rischi e gestione coordinata delle crisi. Una resilienza sostenibile nasce da pratiche quotidiane disciplinate, supportate da controlli tecnologici proporzionati.

7. Discussione finale e valutazione

Esercizio – Discussione riflessiva di consolidamento

Obiettivo: consolidare la comprensione dei concetti principali e favorire l'autovalutazione della responsabilità professionale negli ambienti caratterizzati da rischi di sicurezza digitale.

Modalità: discussione di gruppo

Durata stimata: 20–30 minuti

I partecipanti discutono i seguenti punti di riflessione, collegandoli a situazioni operative reali nel settore turistico:

- Come riconoscere che un problema tecnico o relativo ai dati sta diventando un incidente di sicurezza digitale?

Unità di Formazione 2: La sicurezza digitale nel turismo

- In quale momento un problema dovrebbe essere oggetto di escalation invece di essere gestito individualmente?
- In che modo procedure e documentazione aiutano a operare efficacemente in situazioni di forte pressione?
- Quali comportamenti comunicativi contribuiscono a proteggere la fiducia dei clienti durante e dopo un incidente?
- In che modo il proprio comportamento influenza i colleghi, i clienti e gli esiti del processo di recupero?

Quiz di valutazione finale

Obiettivo: valutare la comprensione teorica e la capacità di applicare i principi affrontati in tutte le componenti dell'Unità 2.

Modalità: valutazione individuale

Durata stimata: 25–35 minuti

Domande:

1. Quando si sospetta un incidente digitale, quale azione dovrebbe essere intrapresa per prima?

- A. Cercare di risolvere il problema autonomamente prima di informare gli altri
- B. Attendere la completa conferma tecnica dell'incidente
- C. Segnalare immediatamente il problema attraverso il canale di segnalazione previsto
- D. Informare gli ospiti prima di avvisare i team interni

Risposta corretta: C

2. Quale concetto affrontato nel corso rafforza maggiormente il senso di responsabilità personale nella sicurezza digitale?

- A. Standard avanzati di crittografia
- B. Principi dello Zero Trust e disciplina dell'escalation tempestiva

- C. Meccanismi di verifica basati su blockchain
- D. Modelli di comunicazione con i media

Risposta corretta: B

3. Perché una comunicazione strutturata riduce l'impatto degli incidenti digitali?

- A. Elimina la necessità di adottare misure tecniche di contenimento
- B. Evita confusione, duplicazione delle azioni ed escalation del danno reputazionale
- C. Sostituisce gli obblighi di notifica previsti dalla normativa
- D. Garantisce che gli incidenti rimangano riservati

Risposta corretta: B

4. Quale comportamento contribuisce maggiormente a ridurre il rischio digitale nelle attività quotidiane?

- A. Condividere le credenziali con colleghi di fiducia
- B. Ignorare piccole anomalie durante i periodi di maggiore lavoro
- C. Segnalare tempestivamente le attività sospette e seguire le procedure previste
- D. Affidarsi esclusivamente al reparto IT per individuare le minacce

Risposta corretta: C

5. Quando un problema operativo dovrebbe essere considerato un potenziale incidente digitale e sottoposto a escalation?

- A. Solo dopo le lamentele dei clienti
- B. Quando esiste un ragionevole sospetto di compromissione dei dati o di uso improprio dei sistemi
- C. Dopo aver ottenuto l'approvazione della direzione
- D. Quando i media iniziano a parlarne

Risposta corretta: B

6. Quale pratica rafforza maggiormente la resilienza digitale nel lungo periodo?

- A. Ripristinare rapidamente i sistemi senza documentare le attività svolte
- B. Analizzare le cause dell'incidente e implementare miglioramenti strutturali
- C. Ridurre al minimo la comunicazione per limitare il danno reputazionale
- D. Considerare ogni incidente come un problema tecnico isolato

Risposta corretta: B

7. Quale comportamento comunicativo contribuisce maggiormente a preservare la fiducia dei clienti durante una crisi?

- A. Fornire immediatamente spiegazioni tecniche dettagliate
- B. Formulare ipotesi sulle possibili cause per apparire trasparenti
- C. Fornire aggiornamenti verificati, coerenti ed empatici
- D. Evitare qualsiasi comunicazione pubblica fino al completamento delle indagini

Risposta corretta: C

8. Quale combinazione descrive meglio un approccio disciplinato alla fase di recupero?

- A. Riavvio rapido dei sistemi, documentazione minima e comunicazione ritardata
- B. Contenimento tecnico, documentazione delle azioni, valutazione degli obblighi normativi e comunicazione coordinata
- C. Scuse pubbliche prima di confermare l'effettivo impatto dell'incidente
- D. Escludere la direzione dalle decisioni relative alla gestione tecnica

Risposta corretta: B

9. Quali DUE fattori consentono più frequentemente a un problema minore di trasformarsi in una crisi digitale?

- A. Ritardo nell'attivazione delle procedure di escalation a causa dell'incertezza
- B. Comunicazione immediata e trasparente alle autorità competenti
- C. Scorciatoie procedurali adottate sotto pressione operativa
- D. Un'efficace segmentazione della rete

Risposte corrette: A e C

10. Quali DUE elementi sono essenziali per garantire la conformità normativa durante un incidente che coinvolge dati personali?

- A. Pubblicare immediatamente un comunicato stampa
- B. Documentare in modo strutturato tutte le azioni intraprese
- C. Valutare il rischio e l'impatto sulle persone interessate
- D. Eliminare internamente i registri delle attività sospette

Risposte corrette: B e C

11. Quali DUE misure riducono più efficacemente la probabilità che un ransomware si propaghi all'interno dei sistemi?

- A. Segmentazione della rete
- B. Condivisione delle credenziali di amministratore solo con la direzione
- C. Backup offline o immutabili
- D. Evitare di coinvolgere specialisti forensi esterni

Risposte corrette: A e C

12. Quali DUE pratiche di comunicazione rafforzano maggiormente la credibilità di un'organizzazione durante una crisi?

- A. Designare un unico portavoce autorizzato

- B. Consentire a più reparti di comunicare autonomamente
- C. Garantire messaggi coerenti su tutti i canali di comunicazione
- D. Divulgare immediatamente dettagli tecnici non ancora verificati

Risposte corrette: A e C

13. Quali DUE comportamenti dimostrano un elevato senso di responsabilità professionale negli ambienti turistici digitalizzati?

- A. Segnalare eventuali anomalie anche in presenza di dubbi
- B. Cercare di risolvere autonomamente sospette violazioni
- C. Seguire le procedure di escalation previste
- D. Aspettare istruzioni esplicite dalla direzione prima di agire

Risposte corrette: A e C

1. Commissione Europea. (2024). *Patto per le competenze dell'UE – Partenariato per le competenze dell'ecosistema del turismo (Aggiornamento della baseline)*. <https://pact-for-skills.ec.europa.eu/>
2. Unione europea. (2015). *Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno (PSD2)*. Gazzetta ufficiale dell'Unione Europea, L 337. <https://eur-lex.europa.eu/eli/dir/2015/2366/oj>
3. Unione europea. (2016). *Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati (Regolamento generale sulla protezione dei dati – GDPR)*. Gazzetta ufficiale dell'Unione Europea, L 119. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
4. Unione europea. (2019). *Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA (Agenzia dell'Unione europea per la cibersicurezza) e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione (Cybersecurity Act)*. Gazzetta ufficiale dell'Unione Europea, L 151. <https://eur-lex.europa.eu/eli/reg/2019/881/oj>
5. Unione europea. (2022). *Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (Direttiva NIS2)*. Gazzetta ufficiale dell'Unione Europea, L 333. <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>
6. Unione europea. (2022). *Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati (Data Governance Act)*. Gazzetta ufficiale dell'Unione Europea, L 152. <https://eur-lex.europa.eu/eli/reg/2022/868/oj>
7. Agenzia dell'Unione europea per la cibersicurezza (ENISA). (2022). *Linee guida sulla cultura della cibersicurezza: aspetti comportamentali della*

cibersicurezza. <https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity>

8. Agenzia dell'Unione europea per la cibersicurezza (ENISA). (2025). *Guida tecnica all'attuazione delle misure di gestione del rischio per la cibersicurezza (Versione 1.0)* [https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA Technical implementation guidance on cybersecurity risk management measures version 1.0.pdf](https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf)
9. Organizzazione internazionale per la normazione (ISO) e Commissione elettrotecnica internazionale (IEC). (2022). *ISO/IEC 27001:2022 – Sicurezza delle informazioni, cibersicurezza e protezione della privacy – Sistemi di gestione della sicurezza delle informazioni – Requisiti*. <https://www.iso.org/standard/27001>
10. Organizzazione Mondiale del Turismo (UNWTO). (s.d.). *Codice etico globale per il turismo*. <https://www.untourism.int/global-code-of-ethics-for-tourism>



 treadsproject.eu

 [treads-project](https://www.linkedin.com/company/treads-project)

 [Treads Project](https://www.facebook.com/TreadsProject)

 [treadsprojecteu](https://www.instagram.com/treadsprojecteu)



Co-funded by the
European Union

Co-funded by the European Union. The opinions and views expressed are solely those of the author(s) and do not necessarily reflect those of the European Union or the Spanish Service for the Internationalization of Education (SEPIE). Neither the European Union nor the granting authority can be held responsible for them