Nell'era digitale in cui viviamo, la minaccia degli attacchi informatici è sempre in agguato, e farsi trovare pronti è indispensabile per affrontarli con maggiore consapevolezza e responsabilità.

L'obiettivo di questo libro è fornire una guida pratica per la gestione degli attacchi informatici, affinchè si possano comprendere le azioni principali da conoscere per farsi trovare pronti.

La Banca dello Stato del Cantone Ticino crede nell'importanza della prevenzione, per dare a tutti i fondamenti per affrontare questa straordinaria trasformazione digitale con maggiore sicurezza.

Fabrizio Cieslakiewicz
Presidente della direzione generale

BancaStato

Fontanaprint

ISBN 978-88-8191-746-4
9 788881 917464

COSA FARE IN CASO DI
Guida pratica per la gestione di attacchi informatici

SUPSI

COSA FARE IN CASO DI

Guida pratica per la gestione di attacchi informatici

Servizio Informatica Forense (SIF)

SUPSI

Stampa e impaginazione:
Fontanaprint
Via Giovanni Maraini 23
CH – 6963 Pregassona
www.fontana.ch
ISBN 978-88-8191-746-4

Le immagini sono state generate con DALL·E 3.

Prima pubblicazione: giugno 2024

La bussola

COSA FARE IN CASO DI

Guida pratica
per la gestione di attacchi informatici

Servizio Informatica Forense (SIF)

SUPSI

1 L'importanza della prevenzione

La sicurezza informatica è diventata una necessità per cittadini, aziende e istituzioni in tutto il mondo. La minaccia di attacchi informatici si è ampliata, diventando più sofisticata e potenzialmente invasiva, colpendo con maggiore frequenza e intensità anche le realtà del Cantone Ticino.

Il Servizio informatica forense (SIF) del Dipartimento tecnologie innovative (DTI) della Scuola universitaria professionale della Svizzera italiana (SUPSI), nato nel 2011, ha raccolto, in quasi quindici anni di attività, molteplici esperienze professionali, svolte sia sul campo investigativo, in collaborazione con le principali Auto-

rità Giudiziarie locali e nazionali, sia nell'ambito della ricerca scientifica svizzera ed europea.

Questo processo si è svolto, e continua a svolgersi, attraverso progetti di ricerca applicata competitivi nel campo dell'informatica forense e della sicurezza informatica a supporto di aziende, istituzioni e cittadini.

Il SIF si avvale della competenza di nove persone qualificate tra ricercatori, collaboratori scientifici e assistenti, ciascuno con una comprovata esperienza professionale di natura interdisciplinare.

L'obiettivo di questo libro è la condivisione pubblica di queste esperienze per il trasferimento della conoscenza, affinché i cittadini, le aziende e le istituzioni del Cantone Ticino possano trarre il massimo vantaggio in ottica di alfabetizzazione digitale.

In particolare, questa guida mira a promuovere un utilizzo consapevole e responsabile delle tecnologie digitali per ciò che riguarda la sicurezza informatica.

Per raggiungere questo obiettivo, è stato adottato uno stile di comunicazione che privilegia la semplicità, limitando l'uso di tecnicismi e acronimi, a favore di un linguaggio chiaro e diretto.

Data la complessità tecnica e l'ampiezza del campo della sicurezza informatica, come pure quello delle investigazioni digitali, il libro si propone in modo pragmatico come un punto di partenza autorevole, piuttosto che come un testo esaustivo di carattere tecnico.

Alessandro Trivilini
Responsabile, Servizio informatica forense
SUPSI

2 **Cosa fare in caso di** richiesta di dati personali?

La richiesta di dati personali può avvenire tramite diversi canali, come ad esempio la posta elettronica, una telefonata oppure attraverso la messaggistica istantanea come gli SMS o WhatsApp.

2.1 A cosa prestare attenzione?

Prima di agire, in caso di richiesta di dati personali, verifica:

Il mittente

- Se la richiesta è avvenuta tramite un messaggio di posta elettronica, assicurati che anche l'indirizzo di provenienza, non solo il nome, appartenga a un contatto di cui puoi verificare l'autenticità. Per esempio, da un'istituzione non aspettarti un indirizzo di posta elettronica con dominio generico @gmail.com o @yahoo.com.
- Se la richiesta è avvenuta tramite una telefonata, SMS o messaggio istantaneo WhatsApp, assicurati

che il numero del mittente, non solo il suo nome, appartenga a un contatto di cui puoi verificare l'autenticità.

Il contenuto

- Controlla nel testo del messaggio la presenza di errori che in genere il mittente non commette. Ad esempio, da un'istituzione non aspettarti un messaggio con errori di battitura.
- Controlla la coerenza dello stile comunicativo del messaggio rispetto a quello che ti aspetti dal mittente. Ad esempio, da un'istituzione non aspettarti uno stile informale.
- Controlla se il tenore della richiesta è tale da metterti pressione psicologica esortandoti ad agire velocemente. Ad esempio, la richiesta ti impone di agire in pochi minuti enfatizzando una situazione di emergenza.

La finalità

- Presta attenzione alla presenza di richieste di dati bancari, credenziali di accesso ai sistemi informatici di qualsiasi tipo, o informazioni di carattere personale. Ad esempio, un'istituzione non ti chiederà mai di fornirle informazioni personali attraverso canali di messaggistica istantanea.

Le tre tipologie di verifica proposte qui sopra forniscono indizi caratterizzanti un messaggio o una chiamata potenzialmente a rischio.

2.2 Come comportarsi?

Indicazioni utili da ricordare in caso di contatto sospetto:

- Non fornire alcuna informazione di carattere personale.
- Verifica attraverso altri canali, diversi da quello con cui hai ricevuto la richiesta, se essa è legittima e autorizzata.
- Se la richiesta coinvolge dispositivi e/o dati aziendali, e non puoi verificare completamente l'autenticità del mittente, per esempio a causa di restrizioni imposte per sicurezza dai sistemi informatici che utilizzi, contatta il tuo superiore diretto.
- Se invece la richiesta coinvolge dispositivi e/o dati privati, e non puoi verificare completamente l'autenticità del mittente, per esempio a causa di restrizioni imposte per sicurezza dai sistemi informatici che utilizzi, contatta la Polizia cantonale per segnalare il caso e ottenere maggiori informazioni.

- In caso di dubbio, per sicurezza non dare seguito alla richiesta in alcun modo.

L'elenco delle indicazioni sopra citato è da considerarsi come punto di partenza, il quale deve, per ovvie ragioni, tener conto del contesto di applicazione.

2.3 L'incidente è capitato, cosa fare?

Nel caso in cui la condivisione di dati personali sia già avvenuta, ai fini della redazione di documentazione oggettiva relativa a quanto accaduto, è opportuno adottare un comportamento consapevole e responsabile, finalizzato ad avvisare tempestivamente:

- Il superiore diretto, in caso di attacco ai dispositivi e/o dati aziendali.
- La Polizia cantonale, in caso di attacco ai dispositivi e/o dati privati.

In particolare, si consiglia di non cancellare alcuna informazione riguardante la richiesta, i contenuti e il con-

tatto, ma di annotare con la massima precisione tutti i dettagli inerenti all'incidente:

- Il mezzo di comunicazione, ad esempio posta elettronica, SMS, telefonata e/o applicazioni di messaggistica istantanea come WhatsApp.
- I dettagli del contatto, ad esempio numero di telefono, indirizzo di posta elettronica, eventuale pseudonimo usato.
- Il contenuto della richiesta o una sua sintesi, ed eventuali dettagli come nomi, luoghi, prodotti, situazioni e altri degni di particolare attenzione.
- In caso di telefonata o messaggi vocali, annotare particolarità della voce, come ad esempio accenti e/o dialetti.
- Quali dati personali sono stati condivisi e se coinvolgono altre persone.

Queste buone pratiche sono utili sia ai cittadini sia alle aziende e alle istituzioni, per raccogliere i dati utili ai fini di un'eventuale denuncia in sede giudiziaria (civile e/o penale).

Sandro Denicolà
Ricercatore, Servizio informatica forense
SUPSI

3 **Cosa fare in caso di** dati inaccessibili a causa di un ransomware?

L'attacco ransomware rappresenta una minaccia crescente per cittadini, aziende e istituzioni. Questo tipo di attacco cifra i dati della vittima richiedendo un riscatto, spesso in criptovaluta, in modo da renderli di nuovo disponibili. Inoltre, può includere minacce di divulgazione di informazioni sensibili all'interno del mercato nero del Dark Web.

3.1 A cosa prestare attenzione?

Solitamente, un attacco ransomware si avvale dell'invio di un messaggio di posta elettronica che include un allegato pericoloso o un link dannoso. Quando l'utente apre l'allegato o clicca sul link, permette al software malevolo di penetrare nel sistema. Una volta infiltrato, questo programma cifra i file, rendendoli inaccessibili.

I messaggi di posta elettronica sospetti si possono riconoscere attraverso:

Il mittente

- Assicurati che l'indirizzo di provenienza, non solo il nome, appartenga a un contatto di cui puoi verificare l'autenticità. Per esempio, da un'istituzione non aspettarti un indirizzo di posta elettronica con un dominio generico come @gmail.com o @yahoo.com.

Il contenuto

- Controlla nel testo del messaggio la presenza di errori che in genere il mittente non commette. Ad esempio, da un'istituzione non aspettarti un messaggio di posta elettronica contenente degli errori di battitura.
- Controlla la coerenza dello stile comunicativo del messaggio rispetto a quello che ti aspetti dal mittente. Ad esempio, da un'istituzione non aspettarti uno stile informale in un messaggio di posta elettronica.
- Controlla se il tenore della richiesta è tale da metterti pressione psicologica esortandoti in brevissimo tem-

po, ad esempio, a scaricare un allegato, a cliccare su un'immagine o un link presente nel messaggio di posta elettronica, enfatizzando una situazione di emergenza.

3.2 Come comportarsi?

Indicazioni utili da ricordare in caso di attacco ransomware, suddivise per fasi:

Prevenzione

Per ridurre il rischio di attacchi ransomware e minimizzarne i danni, puoi adottare questi comportamenti:

- **Backup regolari dei dati:** effettua backup regolari dei tuoi dati importanti. Di norma, sarebbe opportuno avere almeno due copie dei dati, su due diversi supporti posizionati in due luoghi diversi.
- **Aggiornamenti del software:** assicurati che tutti i programmi dei tuoi dispositivi siano costantemente aggiornati alle ultime versioni disponibili.

- **Programmi di sicurezza:** utilizza un antivirus riconosciuto, la cui reputazione sia verificabile e la sua efficacia sia comprovata. Inoltre, mantieni costantemente attivi i sistemi di protezione della rete, come ad esempio Microsoft Defender.

L'elenco sopracitato rappresenta un buon punto di partenza per prevenire e minimizzare i danni dovuti a un attacco ransomware.

Mitigazione

Se il ransomware infettasse il dispositivo rendendo i dati inaccessibili, lo potresti capire attraverso questi segnali:

- **Impossibilità di accedere ai file:** si possono trovare file e cartelle crittografate all'interno del dispositivo infetto, spesso con modifiche ai loro nomi ed estensioni e con impossibilità di accesso.

- **Richiesta di riscatto:** nella maggior parte dei casi, è presente sulla macchina infetta un documento di testo oppure una pagina web che informa l'utente del successo dell'infezione, e fornisce istruzioni per il pagamento del riscatto.

Di conseguenza, segui queste indicazioni su come comportarti:

- **Non pagare il riscatto:** il pagamento non garantisce il recupero dei dati e i malintenzionati potrebbero continuare a estorcere denaro, alimentando così la criminalità organizzata che in un secondo tempo potrebbe tornare a colpire di nuovo.
- **Isola il dispositivo:** in assenza di linee guida aziendali o raccomandazioni istituzionali, disconnetti dalla rete il dispositivo infetto e infine spegnilo, per evitare la possibile propagazione del ransomware.
- **Non cancellare nulla:** conserva tutte le comunicazioni relative all'attacco, come per esempio i mes-

saggi di posta elettronica, oppure tutto ciò che può essere riconducibile all'attacco, e successivamente utile in fase investigativa.

3.3 L'incidente è capitato, cosa fare?

Nel caso in cui l'attacco ransomware abbia reso i dati inaccessibili, ai fini della redazione di documentazione oggettiva relativa a quanto accaduto, è opportuno adottare un comportamento consapevole e responsabile, finalizzato ad avvisare tempestivamente:

- Il superiore diretto, in caso di attacco ai dispositivi e/o dati aziendali.
- La Polizia cantonale, in caso di attacco ai dispositivi e/o dati privati.

In particolare, si consiglia di non cancellare alcuna informazione riguardante la richiesta di riscatto e l'attacco in generale, ma di annotare con la massima precisione tutti i dettagli inerenti all'incidente:

- Il mezzo di comunicazione, ad esempio un messaggio di posta elettronica.
- I dettagli del contatto, ad esempio, nel caso di un messaggio di posta elettronica, l'indirizzo usato ed un eventuale pseudonimo usato.
- Il contenuto della richiesta o una sua sintesi, ed eventuali dettagli come nomi, luoghi, prodotti, situazioni e altre informazioni degne di particolare attenzione.

Inoltre, si considerino le seguenti azioni per completare la fase di ripristino del dispositivo:

- Affidarsi a persone competenti per la rimozione del ransomware e il ripristino dei sistemi. In ambito aziendale e istituzionale avvalersi delle competenze interne messe a disposizione da specialisti informatici autorizzati, mentre in ambito privato avvalersi dei servizi di supporto tecnico offerti da aziende specializzate.
- Se disponibili, utilizzare i backup per ripristinare i dati persi.

Queste buone pratiche sono utili sia ai cittadini sia alle aziende e alle istituzioni, per raccogliere i dati utili ai fini di un'eventuale denuncia in sede giudiziaria (civile e/o penale).

Armando Taglialatela
Assistente, Servizio informatica forense
SUPSI

4 **Cosa fare in caso di** trasmissione dati compromessa da un intruso?

È possibile che i dati che trasmettiamo attraverso la rete Internet, come ad esempio messaggi istantanei, messaggi di posta elettronica, scambio di file, telefonate o videochiamate, o utilizzo di servizi web, vengano "ascoltati" senza il nostro permesso.

In questo caso, stiamo parlando di un attacco informatico in cui qualcuno ascolta, ritrasmette o altera segretamente e senza autorizzazione la comunicazione tra due interlocutori.

Ad esempio tra persone durante una videochiamata o tra una persona e una macchina durante l'utilizzo di servizi web, mentre gli interlocutori sono ignari di ciò che sta accadendo.

4.1 A cosa prestare attenzione?

Verificare se qualcuno sta spiando i dati che trasmetti tramite rete può essere un'operazione molto complicata, specialmente se non sei un esperto nel campo, ed

è spesso riservata al personale informatico opportunamente formato.

Detto ciò, esistono alcune buone pratiche che anche tu puoi seguire, e che non richiedono conoscenze tecniche specifiche, per fare in modo di non incappare in questi problemi:

- **Presta attenzione agli avvisi di sicurezza:** dispositivi e applicazioni inviano avvisi di sicurezza se rilevano attività sospette o potenziali minacce. Spesso, questi includono indicazioni semplici e pratiche per risolvere i vari problemi. È cruciale seguirli con attenzione, assicurandoti che provengano da fonti e applicazioni di cui ti fidi.
- **Osserva comportamenti anomali:** la comparsa sullo schermo di finestre o riquadri inaspettati, interruzioni impreviste di attività online o il rallentamento del computer sono solo alcuni degli indicatori di comportamento anomalo del tuo sistema, che potrebbero segnalare una compromissione.

- **Controlla i link web:** a volte, quando apri un link, potresti non essere indirizzato alla destinazione desiderata, ma piuttosto essere dirottato verso un altro indirizzo del tutto diverso. In tal caso, è probabile che ciò che stai visualizzando non sia il sito che intendevi visitare, ma piuttosto una sua copia di natura illegale. Se, sfortunatamente, inserisci dati personali su questo sito contraffatto, esiste un elevato rischio che questi tuoi dati vengano rubati. È fondamentale prestare molta attenzione alla correttezza dei link e verificare la loro l'autenticità quando navighi in Internet.
- **Osserva accessi non autorizzati:** presta attenzione a eventuali accessi non autorizzati a uno dei tuoi dispositivi o account online, che potrebbero verificarsi in luoghi a te sconosciuti o non familiari. Questi sono segni evidenti di compromissione.

Questi semplici accorgimenti ti permettono di avere maggiore consapevolezza e controllo se qualcuno tentasse di spiare ciò che trasmetti via rete.

4.2 Come comportarsi?

Esistono alcune buone pratiche, ovvero accorgimenti utili da seguire, che garantiscono una maggiore sicurezza nell'invio dei dati attraverso la rete, prevenendo possibili intercettazioni da parte di terzi.

Tra tutte le buone procedure, è importante prestare attenzione ai seguenti comportamenti:

- **Eseguire regolarmente gli aggiornamenti:** aggiornare regolarmente il sistema operativo e le applicazioni installate sul tuo dispositivo ti permette di proteggere il sistema da vulnerabilità conosciute, grazie agli aggiornamenti di sicurezza.
- **Limitare le autorizzazioni delle applicazioni:** limitare le autorizzazioni delle applicazioni installate sul tuo dispositivo ti permette di mantenere sotto controllo quali programmi hanno il permesso di leggere e/o scrivere dati in certe cartelle del sistema, in base al consenso che hai dato in precedenza.

- **Abilitare un "muro tagliafuoco" (firewall):** abilitare il firewall già disponibile nel sistema operativo, come ad esempio Microsoft Defender nel caso di Windows, è una buona soluzione per aiutare a bloccare il traffico dati indesiderato e potenzialmente pericoloso proveniente da Internet, proteggendo così il tuo dispositivo da minacce esterne.
- **Installare un buon programma antivirus:** avere installato sul tuo sistema operativo un buon programma antivirus è fondamentale per proteggere il tuo dispositivo elettronico, affinché i dati non vengano compromessi.
- **Utilizzare una VPN:** l'utilizzo di una VPN (Virtual Private Network) consente di crittografare sia il traffico Internet in entrata sia quello in uscita, rendendo più difficile l'accesso e la lettura dei tuoi dati una volta trasmessi in rete.

- **Evitare di connetterti a reti Wi-Fi pubbliche:** le reti Wi-Fi pubbliche non protette sono spesso soggette all'intercettazione del traffico dati, rendendole un canale privilegiato per questo tipo di attacco.

Ricorda che mantenere sempre aggiornati e protetti i tuoi dispositivi è un fattore tecnico comportamentale essenziale per la sicurezza informatica e per mantenere i tuoi dati al sicuro, anche durante gli scambi via web.

4.3 L'incidente è capitato, cosa fare?

Una volta scoperta una compromissione della sicurezza in una trasmissione dati, si può solamente cercare di riportare il sistema ad uno stato "sicuro" nel minor tempo possibile, in modo da non compromettere successivi scambi di dati via rete.

Inoltre, ai fini della redazione di documentazione oggettiva relativa a quanto accaduto, è opportuno adottare un comportamento consapevole e responsabile, finalizzato ad avvisare tempestivamente:

- Il superiore diretto, in caso di attacco ai dispositivi e/o dati aziendali.
- La Polizia cantonale, in caso di attacco ai dispositivi e/o dati privati.

Ciò può essere realizzato mediante:

- **Isolamento del sistema:** prima di tutto, è necessario disconnettere i dispositivi compromessi dalla rete Internet e dalla rete locale. Questo serve a impedire a chiunque stia controllando i tuoi dispositivi di continuare a farlo, o peggio ancora, di propagarsi ad altri dispositivi.
- **Verifica del sistema:** effettuare una scansione completa del sistema operativo compromesso utilizzando strumenti appositi, spesso integrati nei software antivirus, ti aiuterà a individuare la presenza di eventuali programmi malevoli, spyware o accessi indesiderati installati dall'intruso.

- **Modifica della password:** per garantire l'efficacia di una modifica della password in seguito a una compromissione, è consigliabile cambiare tutte le password degli account in tuo possesso. Assicurati che ciascuna password rispetti i criteri per renderla forte, come ad esempio una lunghezza adeguata, l'inclusione di numeri e caratteri speciali, l'assenza di parole presenti nei dizionari e di date riconducibili a te, e così via.
- **Notifica dell'accaduto:** ricorda di informare tutte le persone coinvolte. In questo modo, potranno prendere le misure necessarie per mitigare i rischi derivanti dalla compromissione della comunicazione. Se l'incidente coinvolge dati privati, non dimenticare di segnalare l'incidente alla Polizia cantonale. Altrimenti, se si tratta di dati aziendali o istituzionali, avvisa il tuo superiore diretto.

Mantenere i tuoi dispositivi il più possibile sicuri, sia in ambito aziendale o istituzionale, sia in ambito privato, aiuta a prevenire la maggior parte dei tentativi di terzi di intercettare le informazioni che stai trasmettendo via web.

Francesco Roberto Dani
Collaboratore scientifico, Servizio informatica forense
SUPSI

5 **Cosa fare in caso di** malfunzionamento improvviso dei servizi web?

Questo tipo di attacco prende di mira uno o più servizi web con un gran numero di richieste al secondo fino a paralizzarli, rendendoli inaccessibili per gli utenti legittimi.

L'interruzione malevola dei servizi web privati, aziendali o istituzionali costituisce una seria minaccia non solo per l'accessibilità, ma anche per la sicurezza dei dati in essi contenuti.

Le principali conseguenze negative riguardano la reputazione, gli aspetti finanziari e la robustezza dell'infrastruttura che ospita i servizi web, siano essi di natura privata, aziendale o istituzionale.

5.1 A cosa prestare attenzione?

Comprendere se l'interruzione sia di natura malevola e identificare le opportune contromisure può essere un'operazione molto complicata per chi non è esperto nel campo.

Esistono alcuni segnali comuni che possono indicare un possibile attacco malevolo ai servizi web, tra cui:

- **Lentezza insolita o servizio irraggiungibile:** se il servizio web diventasse insolitamente lento senza un apparente motivo oppure non fosse più raggiungibile nonostante la buona connessione Internet, potrebbe essere un segno di un attacco malevolo volto a rendere inaccessibile uno o più servizi web.
- **Ripetuti errori di autenticazione:** è fondamentale prestare attenzione ai ripetuti errori di autenticazione, poiché potrebbero indicare ripetuti tentativi di accesso non autorizzato da parte di un potenziale attaccante.

Riconoscere e rispondere prontamente a questi segnali è fondamentale per reagire tempestivamente e per proteggere l'integrità e la disponibilità dei servizi.

5.2 Come comportarsi?

Per ridurre il rischio di un malfunzionamento improvviso di servizi web e per minimizzare i danni, puoi adottare questi comportamenti:

- **Aggiornamenti del software:** mantenere il più possibile aggiornato alle ultime versioni il sistema operativo del dispositivo elettronico, come anche tutte le sue applicazioni installate.
- **Adesione alle linee guida:** se disponibili, agisci seguendo le linee guida aziendali, istituzionali o del fornitore del servizio web, evitando azioni improvvisate.
- **Backup regolari dei dati:** effettuare backup regolari dei dati importanti. Di norma, sarebbe opportuno avere almeno due copie dei dati, su due diversi supporti posizionati in due luoghi diversi.

Seguire questi principi ti aiuterà a mantenere i tuoi dispositivi maggiormente sicuri, sia in ambito aziendale o istituzionale sia in ambito privato, per minimizzare i rischi e i potenziali danni.

5.3 L'incidente è capitato, cosa fare?

Nel caso in cui il servizio web non risulti essere raggiungibile o non funzioni come dovrebbe, ai fini della redazione di documentazione oggettiva relativa a quanto accaduto, è opportuno adottare un comportamento consapevole e responsabile, finalizzato ad avvisare tempestivamente:

- Il superiore diretto, in caso di attacco ai servizi web aziendali.
- La Polizia cantonale, in caso di attacco ai servizi web privati.

Di seguito ecco alcune pratiche consigliate da seguire durante l'attacco:

- Informa tempestivamente dell'accaduto il tuo superiore diretto aziendale o istituzionale, oppure il tuo fornitore di servizi web in caso di compromissione del tuo servizio web privato.

- Prendi nota di tutti i dettagli che potrebbero servire per la creazione del rapporto riguardo all'incidente. Raccogli tutte le informazioni possibili ottenute durante l'attacco, includendo anche la durata e l'intensità, per futuri riferimenti, per scopi legali e di conformità.
- Non continuare a ricaricare il sito compulsivamente. Ricaricare continuamente una pagina web non aiuterà infatti a risolvere il problema, e, anzi, potrebbe contribuire a sovraccaricare ulteriormente il servizio.
- In caso di attacco a servizi web aziendali o istituzionali, se disponibile, segui le indicazioni contenute nel piano di risposta agli incidenti. In caso contrario, prevedi di comunicare tempestivamente ai destinatari dei servizi web in questione, attraverso canali alternativi e sicuri, l'indisponibilità di tale servizio e tutti gli aggiornamenti che lo riguardano, fino al ripristino dello stesso.

Affrontare un attacco ai servizi web richiede una risposta rapida e coordinata, sia a livello gestionale sia tecnologico. Prevenire, riconoscere e rispondere prontamente è fondamentale per proteggere l'integrità e la disponibilità dei servizi online caratterizzanti l'identità dell'azienda, dell'istituzione o tua privata.

Queste buone pratiche sono utili sia ai cittadini sia alle aziende e alle istituzioni, ai fini di un'eventuale denuncia in sede giudiziaria (civile e/o penale).

Sonia Cenceschi
Ricercatrice, Servizio informatica forense
SUPSI

6 **Cosa fare in caso di** file allegati sospetti?

Un file allegato sospetto può essere inviato tramite diversi canali, come ad esempio un messaggio di posta elettronica, oppure con la messaggistica istantanea come gli SMS o WhatsApp.

6.1 A cosa prestare attenzione?

Prima di intraprendere qualsiasi azione, verifica i seguenti aspetti:

Il mittente

- Se il file allegato è stato inviato tramite un messaggio di posta elettronica, assicurati che anche l'indirizzo di provenienza, non solo il nome, appartenga a un contatto di cui puoi verificare l'autenticità. Per esempio, da un'istituzione non aspettarti un indirizzo di posta elettronica con un dominio generico come @gmail.com o @yahoo.com.
- Se il file allegato è stato inviato tramite servizi di messaggistica istantanea, come WhatsApp o SMS,

assicurati che il numero del mittente, non solo il suo nome, appartenga a un contatto di cui puoi verificare l'autenticità.

Il contenuto

- Controlla la presenza di errori di battitura o discrepanze con lo stile di comunicazione abituale del mittente nel testo del messaggio di posta elettronica che accompagna il file. Ad esempio, da un'istituzione non aspettarti un messaggio con errori di battitura.
- Controlla l'estensione del file in allegato. Alcune estensioni, come .exe, .jar, .cpl, .com, .bat, .msi, .js, .wsf, .pdf, .zip o quelle relative a documenti come Word (.doc, .docx), Excel (.xls, .xlsx) e PowerPoint (.ppt, .pptx), possono essere associate alla diffusione di software dannosi o malware. Ad esempio, da un'istituzione non aspettarti di ricevere file che possono essere eseguiti direttamente sul computer o altri tipi di file con particolari estensioni, come .com, .bat, .pif.

- Controlla l'estensione dell'allegato. Molte volte un attaccante cambia l'estensione per mascherare la vera tipologia del file. Ad esempio, un file chiamato "esempio.exe.jpg" non è un'immagine come si potrebbe pensare in un primo momento, ma bensì un programma eseguibile.

La finalità

- Presta attenzione se il messaggio di posta elettronica o se il messaggio istantaneo ti chiede di scaricare, cliccare o aprire un file allegato sospetto, invocando la risoluzione di un "problema urgente".

Le tre tipologie di verifica proposte forniscono indizi caratterizzanti un file allegato potenzialmente malevolo.

6.2 Come comportarsi?

Indicazioni utili da ricordare in caso di un messaggio contente un file allegato sospetto:

- Prima di aprire l'allegato, verifica la legittimità del messaggio contattando il mittente con un altro mezzo, ad esempio una telefonata.
- Prima di aprire l'allegato, salvalo sul computer e controllalo con un software antivirus riconosciuto, la cui reputazione sia verificabile e la sua efficacia sia comprovata, o con strumenti online, come VirusTotal[1].
- In caso di dubbio, anche se il software antivirus indica che il file allegato è sicuro, è meglio non aprirlo se ti sembra comunque sospetto.
- Se ricevi un allegato con estensione .zip devi fare molta attenzione ed essere cauto. Potrebbe nascondere file eseguibili che sembrano documenti appa-

[1] https://www.virustotal.com/old-browsers/

rentemente innocui, come dei semplici file Word o PDF, ma che in realtà sono malevoli.

- In caso di dubbio, se ritieni che il file allegato ha un'estensione sospetta, evita di scaricarlo, aprirlo e/o eseguirlo.
- Diffida dai messaggi di posta elettronica o dai messaggi istantanei con oggetto "urgente" che ti spingono ad aprire rapidamente e sotto pressione il file. Inoltre, presta attenzione a eventuali richieste insolite nel messaggio. Gli aggressori spesso sfruttano l'urgenza per manipolare i destinatari e indurli ad aprire allegati dannosi.
- Se non puoi verificare completamente l'autenticità del mittente, a causa di restrizioni di sicurezza imposte dai sistemi informatici aziendali o istituzionali, contatta il tuo superiore diretto. Da privato, invece, se non sai come effettuare tale verifica, rivolgiti a una persona esperta e fidata.

L'elenco delle indicazioni sopra citato è da considerarsi come punto di partenza, il quale deve, per ovvie ragioni, tener conto del contesto di applicazione.

6.3 L'incidente è capitato, cosa fare?

Nel caso in cui l'apertura di un file allegato malevolo sia già avvenuta, ai fini della redazione di documentazione oggettiva relativa a quanto accaduto, è opportuno adottare un comportamento consapevole e responsabile, finalizzato ad avvisare tempestivamente:

- Il superiore diretto, in caso di attacco ai dispositivi e/o dati aziendali.
- La Polizia cantonale, in caso di attacco ai dispositivi e/o dati privati.

In particolare, si consiglia di non cancellare alcuna informazione riguardante il file allegato, i contenuti e il contatto, ma di annotare con la massima precisione tutti i dettagli inerenti all'incidente:

- Il mezzo di comunicazione, ad esempio posta elettronica, SMS o applicazioni di messaggistica istantanea, come WhatsApp.
- I dettagli sul mittente o sulla fonte da cui è arrivato il file sospetto. Ad esempio, indirizzo di posta elettronica, o numero telefonico.
- Il tipo di file malevolo allegato, come la sua estensione.
- Il comportamento del file malevolo nel caso sia stato erroneamente e involontariamente aperto, ad esempio se ha cifrato i file o bloccato l'accesso al sistema.
- Eventuali sintomi rilevati dopo l'apertura involontaria del file, come messaggi di errore o impossibilità di accedere ai file.
- Se pertinente, come ad esempio in caso di attacco ransomware, annotare eventuali richieste di riscatto e modalità di pagamento proposte dai criminali informatici.

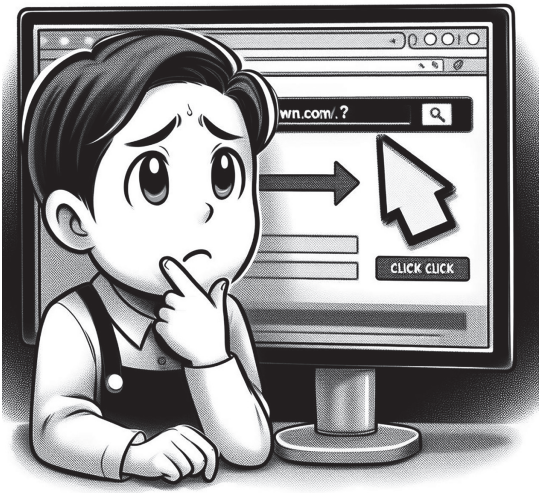
- Se inerente, annotare quali dati personali sono stati condivisi e se coinvolgono altre persone.

Queste buone pratiche sono utili sia ai cittadini sia alle aziende e alle istituzioni, per raccogliere i dati utili ai fini di un'eventuale denuncia in sede giudiziaria (civile e/o penale).

Elisa Colletti

Collaboratrice scientifica, Servizio informatica forense
SUPSI

7 **Cosa fare in caso di** link sospetti?



Link sospetti possono arrivare attraverso diversi canali, come la posta elettronica, la messaggistica istantanea, per esempio WhatsApp, oppure tramite SMS.

I link contenuti in questi messaggi sono "camuffati" in modo da apparire legittimi. In realtà, la pagina web che si apre appartiene ad un sito fittizio, allestito dall'attaccante, che spesso è indistinguibile da quello autentico.

Molto spesso la pagina web illegittima richiede di inserire le credenziali di accesso relative all'istituzione per la quale si spaccia di essere. Così facendo, si consegnano le proprie credenziali di accesso a coloro che stanno operando l'attacco informatico sulla pagina web clonata.

È quindi essenziale capire se il messaggio è legittimo e se il link contenuto in esso porta effettivamente al reale indirizzo Internet dell'organizzazione con la quale si è convinti di avere a che fare.

7.1 A cosa prestare attenzione?

Prima di fare click sul link, verifica:

Il mittente

- Se la richiesta è avvenuta tramite un messaggio di posta elettronica, assicurati che anche l'indirizzo di provenienza, non solo il nome, appartenga a un contatto di cui puoi verificare l'autenticità. Per esempio, da un'istituzione non aspettarti un indirizzo di posta elettronica con un dominio generico come @gmail.com o @yahoo.com.
- Se la richiesta è avvenuta tramite SMS o messaggio istantaneo, come WhatsApp, assicurati che il numero del mittente, non solo il suo nome, appartenga a un contatto di cui puoi verificare l'autenticità.

Il contenuto

I link possono essere artefatti in vari modi, così da apparire legittimi. È quindi importante conoscere le tecniche più comunemente usate dagli attaccanti:

- Controlla nel testo del messaggio, in cui è presente il link sospetto, la presenza di errori che in genere il mittente non commette. Ad esempio, da un'istituzione non aspettarti un messaggio con errori di battitura.
- Controlla la coerenza dello stile comunicativo del messaggio rispetto a quello che ti aspetti dal mittente. Ad esempio, da un'istituzione non aspettarti uno stile informale.
- Controlla se il tenore della richiesta è tale da metterti pressione psicologica esortandoti ad agire velocemente. Ad esempio, la richiesta ti sollecita a cliccare sul link sospetto, entro pochi minuti, enfatizzando una situazione di emergenza.

La finalità

- Presta attenzione se il messaggio ti chiede di usare il link per evitare un "problema urgente". Ad esempio, un'istituzione non ti chiederà mai di effettuare un'operazione di questo tipo tramite messaggio. In particolare, il messaggio potrebbe sollecitarti a cliccare sul link per evitare il blocco del conto corrente o della carta di credito, oppure potrebbe avvisarti di un'intrusione informatica che deve essere urgentemente bloccata, richiedendo un intervento immediato, come il cambio della password (sempre usando il link inserito nel messaggio). Messaggi di questo tipo non sono mai autentici.

7.2 Come comportarsi?

Indicazioni utili da ricordare in caso di messaggio contenente un link sospetto:

- Salva nei preferiti i servizi che utilizzi più spesso, come ad esempio quello del tuo e-banking. In questo modo avrai un link diretto al servizio, senza dover passare da Google.
- Verifica attraverso altri canali, diversi da quello con cui hai ricevuto la richiesta, se essa è legittima e autorizzata.
- Se non puoi verificare completamente l'autenticità del mittente, a causa di restrizioni di sicurezza imposte dai sistemi informatici aziendali o istituzionali, contatta il tuo superiore diretto. Da privato, invece, se non sai come effettuare tale verifica, rivolgiti a una persona esperta e fidata.
- In caso di dubbio, per sicurezza non fare click su link.

L'elenco delle indicazioni sopra citato è da considerarsi come punto di partenza, il quale deve, per ovvie ragioni, tener conto del contesto di applicazione.

Le tecniche per mascherare un link malevolo in modo tale da far risultare che sia legittimo sono diverse. Per difendersi è essenziale seguire le seguenti regole:

- Non ti basare sul testo visibile per valutare dove il link punta davvero. È necessario visualizzare l'indirizzo Internet. Attraverso la barra di stato, che di solito è posta nella parte bassa della finestra del browser web, è possibile visualizzare l'indirizzo del link sul quale la freccia del mouse si trova. Basta quindi spostare la freccia su un link, **senza fare click**, e osservare la barra di stato.
- I programmi di posta elettronica hanno anch'essi la possibilità di visualizzare l'indirizzo dei link contenuti nei messaggi, o tramite una barra di stato dal funzionamento simile a quella presente nei browser web,

oppure attraverso un tooltip. Un tooltip è un piccolo riquadro che compare quando la freccia del mouse si trova su un link e rimane immobile su di esso per alcuni secondi, e visualizza l'indirizzo del link stesso.

- Leggi bene l'indirizzo visualizzato dalla barra di stato o nel tooltip. Molto spesso il link malevolo ha un carattere o un dominio differente da quello legittimo, ma che assomiglia molto all'originale.
- I link contenuti in SMS e messaggi WhatsApp sono più difficili da verificare. In generale, a meno che il mittente non sia assolutamente certo, e la ragione del messaggio assolutamente nota e legittima, non fare click sui link contenuti in questo tipo di messaggi.

7.3 L'incidente è capitato, cosa fare?

Nel caso in cui hai fatto click su un link che si è rivelato malevolo, è opportuno adottare un comportamento consapevole e responsabile, finalizzato ad avvisare tempestivamente:

- Il superiore diretto, in caso di attacco ai dispositivi e/o dati aziendali.
- La Polizia cantonale, in caso di attacco ai dispositivi e/o dati privati.

In particolare, si consiglia di non cancellare alcuna informazione riguardante la richiesta, i contenuti e il contatto, ma di annotare con la massima precisione tutti i dettagli inerenti all'incidente:

- Il mezzo di comunicazione, ad esempio posta elettronica, SMS, e applicazioni di messaggistica istantanea, come WhatsApp.

- I dettagli del contatto, ad esempio numero di telefono, indirizzo di posta elettronica, e/o eventuale pseudonimo usato.
- Il contenuto della richiesta o una sua sintesi, ed eventuali dettagli come nomi, luoghi, prodotti, situazioni e altri degni di particolare attenzione.
- Le informazioni caratterizzanti il link malevolo. È utile in caso di denuncia per risalire a chi ha registrato il dominio a cui appartiene il link.
- Qual è stata l'operazione effettuata nella pagina web che si è aperta a seguito del click su link malevolo. Per esempio, se si sono inserite le credenziali di accesso ad una certa istituzione.

Inoltre, tieni in considerazione anche i seguenti aspetti:

- Se, come succede spesso, l'operazione è stata quella di inserire le credenziali di accesso ad una certa organizzazione, la difesa immediata che puoi adottare è accedere al sito web autentico e ufficiale dell'orga-

nizzazione in questione (usando un indirizzo noto), e cambiare immediatamente la tua password. Inoltre, segnala l'accaduto all'organizzazione tempestivamente tramite il loro modulo di contatto ufficiale.

- Se si tratta di dati compromessi relativi a una tua carta di credito, invece, agisci come se si trattasse di un furto tradizionale fisico di tale carta.

La regola di base per difendersi da questo tipo di attacco è: prima di fare click sul link contenuto in un messaggio, accertarti che esso sia autentico e che l'indirizzo contenuto nel link sia legittimo.

Queste buone pratiche sono utili sia ai privati cittadini sia alle aziende e alle istituzioni, utili ai fini di un'eventuale denuncia in sede giudiziaria (civile e/o penale).

Roberto Tedesco
Ricercatore, Servizio informatica forense
SUPSI

8 **Cosa fare in caso di** ritrovamento di pennetta USB sconosciuta?

Le pennette USB, così come tutti i dispositivi di memoria che consentono di archiviare file, permettono di memorizzare e diffondere anche programmi potenzialmente malevoli.

Il costo estremamente contenuto e l'enorme diffusione di questi dispositivi hanno consentito la propagazione di una nuova serie di attacchi che prevedono come punto di ingresso un dispositivo USB direttamente collegato al computer bersaglio.

L'enorme progresso tecnologico nel campo della miniaturizzazione dei componenti elettronici ha consentito di mascherare all'interno di dispositivi apparentemente innocui, come ad esempio cavetti per la ricarica, dei veri e propri micro-computer.

8.1 A cosa prestare attenzione?

Prima di collegare un dispositivo USB al computer tieni in considerazione le seguenti indicazioni:

Origine del dispositivo

- Guarda con attenzione la pennetta USB per controllare se la riconosci.
- Se non la riconosci, informati domandando se qualcun altro di cui ti fidi la riconosce.
- Se non puoi accertare l'origine del dispositivo, è meglio non collegarla al computer.

Tipologia del dispositivo

- Prima di collegare un dispositivo USB al computer accertati della sua provenienza. Questo accorgimento è valido non solo per le pennette USB, ma anche per tutte le tipologie di dispositivi USB, come ad esempio tastiere, mouse e cavi.

Contenuto del dispositivo

- Anche se riconosci il dispositivo USB, presta comunque sempre attenzione ai file contenuti al suo interno quando lo colleghi al computer. Se ad esempio trovi dei nuovi file inaspettati, meglio eseguire una scansione del dispositivo con un antivirus.

Le tre tipologie di verifica proposte forniscono delle indicazioni a cui prestare attenzione nei confronti di un dispositivo USB.

8.2 Come comportarsi?

Indicazioni utili da ricordare in caso di ritrovamento di una pennetta o di un dispositivo USB:

- In caso di ritrovamento di una pennetta o di un dispositivo USB di cui non conosci la provenienza, non collegarlo al tuo computer.
- Se hai smarrito una pennetta USB e poi l'hai ritrovata, nonostante tu la considerassi dispersa, è opportuno trattarla con molta prudenza. Esegui una pulizia completa del dispositivo tramite l'opzione di formattazione che il sistema operativo ti mette a disposizione. Ricorda che non è sufficiente eliminare i file presenti su di esso, ma è necessario eseguire una formattazione totale, completa e approfondita.

L'elenco delle indicazioni sopra citato è da considerarsi come un punto di partenza, il quale deve per ovvie ragioni tener conto del contesto di applicazione.

8.3 L'incidente è capitato, cosa fare?

Nel caso in cui fosse stato collegato al computer un dispositivo USB rivelatosi malevolo, si rivela opportuno adottare un comportamento consapevole e responsabile atto alla documentazione oggettiva di quanto accaduto.

In particolare, si consiglia di non cancellare nessun file presente sul dispositivo USB e di scollegarlo immediatamente. Successivamente si consiglia di annotare con la massima precisione tutti i dettagli inerenti all'incidente, come:

- Dove è stato trovato il dispositivo USB.
- Di che tipo di dispositivo USB si tratta, ad esempio, una pennetta USB, un mouse, un cavo di alimentazione.
- Dettagli sulla dinamica che hanno preceduto la connessione del dispositivo USB al computer.
- Se è il caso, il tipo di file presente sul dispositivo USB che è stato aperto, come la sua estensione e il suo nome.

- Comportamento del file malevolo una volta aperto, ad esempio se ha cifrato i file presenti sul computer o bloccato l'accesso al sistema.
- Eventuali sintomi rilevati dopo l'apertura del file, come messaggi di errore o impossibilità di accedere ai file.
- Se pertinente, come ad esempio in caso di attacco ransomware, annotare eventuali richieste di riscatto e modalità di pagamento proposte dai criminali informatici.

Queste buone pratiche sono utili sia ai privati cittadini sia alle aziende e alle istituzioni, per raccogliere i dati utili ai fini di un'eventuale denuncia in sede giudiziaria (civile e/o penale).

Nicolas Tagliabue
Collaboratore scientifico, Servizio informatica forense
SUPSI

9 Come scrivere un rapporto con i crismi dell'informatica forense?

Scrivere un rapporto post-incidente che documenti in modo corretto e completo tutto ciò che ha riguardato l'attacco informatico subìto richiede molta attenzione e un approccio sistematico, fondato sul principio della riproducibilità delle prove e delle informazioni.

Questo significa che tutto ciò che viene scritto non solo deve essere comprensibile da chiunque senza alcuna conoscenza tecnica particolare, ma deve anche fornire in modo preciso e dettagliato le informazioni utili affinché, se necessario, chiunque con le dovute competenze possa risalire all'autorevolezza dei risultati ottenuti.

Sebbene siamo entrati nell'era dell'Intelligenza Artificiale Generativa, in cui i testi possono essere scritti con il supporto linguistico degli algoritmi, è opportuno chiarire che un rapporto di questo tipo non rappresenta la narrazione di una storia, bensì il resoconto dettagliato di fatti che soltanto chi li ha dovuti affrontare e gestire può conoscere, spiegare e descrivere.

Affermazioni generiche ottenute grazie all'Intelligenza Artificiale Generativa, per quanto linguisticamente corrette, potrebbero risultare inutili ai fini del rapporto documentale e in sede probatoria, forse anche controproducenti.

Lo stile comunicativo necessario per redigere un rapporto oggettivo (post-incidente) valido in sede probatoria per una denuncia in sede giudiziaria, sia di carattere penale sia civile, diventa quindi un'arte da imparare, seguendo i principi fondamentali suggeriti dall'informatica forense e utilizzando una modalità espressiva semplice e chiara.

Per prima cosa, per scegliere le parole giuste da utilizzare nel rapporto è importante non confondere il significato con il significante.

Ogni parola è composta di due facce inseparabili della stessa medaglia.

La prima è il **significante**, ossia la parola scritta o pronunciata come elemento percepibile (recepibile) con i nostri sensi cognitivi.

La seconda invece è il **significato**, ossia l'elaborazione e l'interpretazione personale di ciò che è letto e ascoltato. O meglio, l'immagine mentale che siamo in grado di associare al significante.

Ricorda che ogni parola che scrivi, pronunci, ricevi e ascolti è caratterizzata da questi due valori.

A questo punto la domanda che sorge spontanea è: "*Che significato attribuirà l'altro individuo al nostro significante (a ciò che comunichiamo)?*"

La risposta è una sola, e dipende dalle sue competenze e da quanto è chiara e precisa la descrizione:

- Dei fatti accaduti.
- Delle azioni intraprese.
- Dei problemi riscontrati.

- Delle soluzioni adottate.
- Dei risultati ottenuti.

Un rapporto post-incidente informatico non viene redatto solo per le persone che hanno affrontato e, si spera, risolto l'incidente, ma piuttosto per tutti coloro che sono chiamati successivamente a prendere decisioni riguardanti quanto accaduto, con un'ottica orientata alla responsabilità.

Essi devono poter comprendere senza l'ausilio di alcun supporto quanto accaduto, nel rispetto di tutti i cinque punti sopra elencati.

A questo proposito, e con questo grado di consapevolezza, l'Intelligenza Artificiale Generativa può essere considerata come uno strumento di aiuto per definire uno stile comunicativo semplice e privo di errori linguistici, ma dev'essere sostenuto dai seguenti principi fondamentali:

- **Verificabilità:** tutte le persone autorizzate dovrebbero essere in grado di valutare e comprendere le azioni riportate nel documento. Questo è possibile soltanto documentando tutte le azioni prese, dalla più importante a quella data per scontata. In particolare, è importante spiegare perché si è scelto di agire in un certo modo. Questa prassi consente una valutazione oggettiva da parte di persone esterne, come ad esempio un membro del Consiglio di Amministrazione, un Avvocato oppure un Procuratore Pubblico, per vedere se hanno seguito le procedure giuste.

- **Ripetibilità:** la ripetibilità di ciò che viene inserito del rapporto è garantita quando gli stessi risultati ottenuti sono prodotti nelle seguenti condizioni:
  - Utilizzando la stessa procedura e metodo di misurazione/descrizione.
  - Utilizzando gli stessi strumenti e nelle stesse condizioni (interne ed esterne).
  - Può essere ripetuto in qualsiasi momento dopo il risultato finale.

Una persona qualificata dovrebbe essere in grado di eseguire tutti i processi descritti nella documentazione e ottenere gli stessi risultati, senza bisogno di guida o interpretazione.

Chi redige il documento dev'essere consapevole che potrebbero esserci circostanze in cui potrebbe non essere possibile ripetere le attività che hanno portato a certi risultati risolutivi del problema. In questi casi, è opportuno descrivere in dettaglio le motivazioni senza trarre alcuna decisione di carattere personale (soggettiva).

- **Riproducibilità:** la riproducibilità delle attività riportate in un rapporto è stabilita quando le stesse attività sono prodotte nelle seguenti condizioni:
  - Utilizzando lo stesso metodo di misurazione.
  - Utilizzando strumenti diversi e in condizioni diverse.
  - Possono essere riprodotte in qualsiasi momento dopo la consegna del rapporto.

Le necessità di riprodurre i risultati variano in base a molti fattori, come ad esempio le regole e le normative in vigore a livello legale. Per cui, la persona incaricata di effettuare la riproduzione dovrà trovare nel documento anche le informazioni utili sulle condizioni applicabili da seguire.

- **Giustificabilità:** chi ha la responsabilità di redigere il rapporto post-incidente dovrebbe essere in grado di giustificare tutte le azioni e i metodi utilizzati nella gestione delle potenziali prove digitali. La giustificazione può essere ottenuta dimostrando che la decisione era la scelta migliore per ottenere tutte le potenziali prove digitali documentate. Questo è necessario per dare la possibilità ad altri esperti incaricati nel corso delle indagini, in totale trasparenza, di poter riprodurre e convalidare con successo le azioni e i metodi utilizzati.

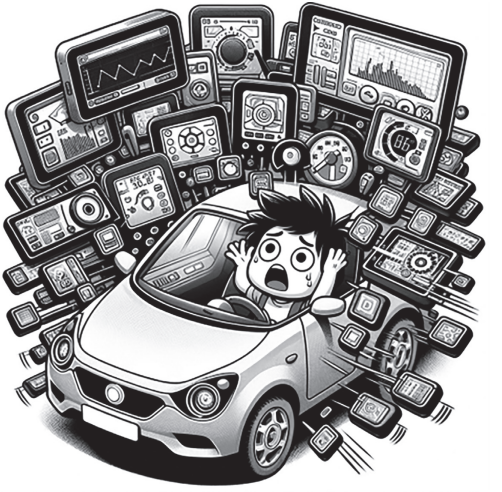
Scrivere un rapporto post-incidente non può considerarsi come una procedura predefinita tratta da un modello preconfezionato, in quanto ogni caso ha le sue peculiarità.

Nonostante ciò, è fondamentale avvalersi di un buon metodo per farlo, onde evitare di perdere informazioni importanti, o, peggio ancora, che in sede probatoria

le informazioni contenute nel documento, per quanto rappresentative, risultino il frutto di un'interpretazione soggettiva non validabile, non riproducibile e non giustificabile.

Alessandro Trivilini
Responsabile, Servizio informatica forense
SUPSI

10 Buone pratiche di igiene digitale



Ti è mai capitato di dover lasciare la tua auto in un quartiere poco sicuro?

In queste situazioni, solitamente scegliamo un posto ben visibile: se possibile sotto un lampione, togliamo tutti gli oggetti di valore, nascondiamo le cose che potrebbero essere allettanti, verifichiamo che i finestrini siano ben chiusi e chiudiamo l'auto!

Perché?

Perché "l'occasione rende l'uomo ladro" e noi non vogliamo essere privati dei nostri beni, né tanto meno ritrovarci con l'auto danneggiata.

Seguendo questa metafora, Internet potrebbe rivelarsi come un quartiere poco sicuro. Adottare delle buone pratiche di igiene digitale significa fare del proprio meglio per evitare di essere danneggiati.

Poiché in questo caso non possiamo scegliere il quartiere, non abbiamo altra scelta che prendere tutte le

contromisure di sicurezza necessarie e considerarle alla stregua di una prassi da seguire, come abitudine.

Come base di partenza per una buona igiene digitale bisognerebbe sempre impostare un sistema di autenticazione per accedere o sbloccare i tuoi dispositivi, compresi i dischi interni per i computer ed eventuali dischi esterni o chiavette USB, e dotarti di un "allarme", ovvero di un buon antivirus.

10.1 Gestione delle password

Perché è importante usare password robuste?

Una password si definisce debole se è facile da indovinare. Utilizzare una password debole sarebbe come usare un pezzo di nastro adesivo per chiudere la porta dell'auto, anziché chiuderla bene a chiave. Per analogia, utilizzare una password troppo semplice per accedere al computer non costituisce un meccanismo di sicurezza sufficiente, e potrebbe compromettere anche altri account presenti sullo stesso, o, addirittura, tutta una struttura informatica lavorativa.

Come posso creare password robuste e gestirle in modo sicuro?

Di norma è raccomandabile usare password con almeno 12 caratteri che comprendano una o più maiuscole, minuscole, numeri e simboli.

Una strategia efficace è quella di selezionare almeno cinque parole, anche inesistenti, in maniera casuale e di creare una password, combinando tutte queste parole in aggiunta a numeri e caratteri speciali.

È importante che le parole scelte siano casuali: non utilizzare per esempio il nome del tuo animale domestico, la data di nascita di tuo figlio, la tua squadra sportiva del cuore o tutte quelle informazioni personali facilmente individuabili.

Le password, in aggiunta, devono essere differenti in maniera sostanziale per ogni account. In questo modo, se qualcuno riesce a individuare o rubare una password non potrà riutilizzarla per accedere anche ad altri account di tua proprietà.

Vi sono vari modi per creare e memorizzare password sicure. Alcune applicazioni, chiamate Password Manager (gestori di password), generano password robuste, e le memorizzano al sicuro sul dispositivo dove sono state installate.

Cos'altro posso fare per rafforzare la sicurezza dopo aver reso più robusta la mia password?

Per rafforzare ulteriormente la sicurezza dei tuoi account, laddove è previsto, attiva l'autenticazione a più fattori (MFA). Il principio dell'autenticazione a più fattori segue il concetto di "qualcosa che io conosco" (una password) combinato con "qualcosa che io posseggo" (un dispositivo). Con questo principio si evita lo scenario in cui, un attaccante che sia riuscito ad avere possesso della sola password, possa autenticarsi, poiché avrebbe bisogno anche del dispositivo in cui arrivano o vengono generati i codici necessari per completare l'accesso al sistema.

Come funziona l'autenticazione a più fattori?

L'autenticazione a più fattori prevede generalmente:

1. Una password da ricordarsi.
2. Un codice temporaneo e sempre differente, perché generato al momento del tentativo di accesso.

Esistono differenti metodi per ricevere il codice temporaneo, ma i principali sono:

- Invio di un SMS ad un numero telefonico prestabilito.
- Invio di un messaggio di posta elettronica ad un indirizzo prestabilito.
- Invio di una notifica di accesso da convalidare sul proprio dispositivo.
- Utilizzo di un'applicazione generatrice di codici temporanei, come ad esempio Authy o Google Authenticator.

Per attivare l'autenticazione a più fattori, generalmente è necessario accedere alla sezione delle impostazioni dell'applicazione o del sito web per cui desideri attivare questa funzione. Qui, potrai selezionare il metodo di autenticazione che preferisci o che trovi più pratico.

Una volta attivata l'autenticazione a più fattori, nel momento in cui desideri accedere al sito web o all'applicazione con le tue credenziali, inserendo il tuo nome utente e password, ti verrà richiesto anche di inserire un codice temporaneo di sicurezza, che ti verrà comunicato tramite uno dei metodi sopracitati.

10.2 Aggiornamento del software

Perché è importante aggiornare regolarmente il sistema operativo e le applicazioni?

L'aggiornamento del tuo sistema operativo e di tutte le applicazioni che usi dovrebbe essere una procedura regolare. Esattamente come si fa con un'automobile con la manutenzione ordinaria e con i servizi preparatori necessari al collaudo.

Cosa implica aggiornare regolarmente il sistema operativo e le applicazioni?

Gli aggiornamenti automatici possono farti storcere il naso, perché richiedono tempo e interrompono le tue attività lavorative.

Ma, sempre pensando alla metafora dell'automobile, se il concessionario dovesse improvvisamente richiamare il veicolo a causa di un problema di fabbricazione, come reagiresti?

Anche per gli aggiornamenti del sistema operativo e delle sue applicazioni, il ragionamento è analogo: a seguito di una vulnerabilità o di un malfunzionamento è opportuno agire tempestivamente con gli aggiornamenti.

Perché è opportuno rimuovere le applicazioni che non usi?

Le applicazioni che non usi da tempo probabilmente saranno obsolete, e dunque vulnerabili in termini di sicurezza. Tali applicazioni possono infatti introdurre opportunità di accesso non autorizzato al dispositivo elettronico da parte di malintenzionati.

10.3 Backup

Che cosa è il backup dei dati?

Il backup dei dati consiste nel copiare file e cartelle in modo automatico, da un dispositivo a un disco di archiviazione esterno e cifrato, o al Cloud, per poterli ripristinare in caso di perdita dei dati originali.

Di regola, per avere un sufficiente grado di sicurezza che i tuoi dati siano al sicuro, puoi utilizzare la seguente strategia: avere almeno due copie dei dati, su due diversi supporti, posizionati in due luoghi diversi.

Spesso gli utenti eseguono il backup dei dati ma poi eliminano gli originali per risparmiare spazio. Con questo comportamento si annulla il principio stesso del backup, ossia di avere una o più copie di sicurezza in aggiunta ai dati originali.

10.4 Accorgimenti tecnici e comportamentali

Perché utilizzare una porta USB pubblica potrebbe essere dannoso?

Da diversi anni le agenzie di cibersicurezza mettono in guardia dall'uso di caricabatterie e cavi pubblici, ad esempio presenti sui mezzi di trasporto e negli aeroporti, per ricaricare telefoni cellulari o computer portatili. Questo perché un attaccante potrebbe sfruttare la tua necessità di corrente per infettare i tuoi dispositivi, attraverso l'esecuzione di malware a tua insaputa.

Se voglio collegarmi ad una rete Wi-Fi pubblica, quali accorgimenti devo adottare per proteggermi?

Le reti Wi-Fi pubbliche, ossia che non hanno nessun meccanismo di autenticazione, sono spesso utilizzate dagli attaccanti per intercettare il traffico dati. Se non puoi evitare di collegarti ad una rete Wi-Fi pubblica, allora è necessario adottare delle contromisure per proteggere la sicurezza e la riservatezza della tua

connessione. Ciò è possibile, per esempio, attraverso l'utilizzo di una VPN che "inscatola" la tua connessione, proteggendola.

Come posso controllare che la mia navigazione sia sicura?

Per essere certi che la navigazione su un sito web sia sicura, in particolare dove è richiesta un'autenticazione, come ad esempio sul sito della banca o della casella di posta elettronica, è possibile eseguire tre verifiche principali:

- Verifica che nella barra degli indirizzi, ossia dove viene visualizzato l'indirizzo del sito web, compaia esattamente l'indirizzo del sito a cui ti vuoi collegare.
- Verifica che nella barra degli indirizzi, a fianco dell'indirizzo del sito, non ci sia un avviso o un'icona che avverta che il sito non è sicuro.
- Verifica che l'indirizzo web visualizzato nella barra degli indirizzi, inizi con http**s**:// (dove la "**s**" sta per "sicuro", ed è importante che ci sia).

Posso fare altro per rendere sicura la navigazione?

Non cliccare su link di cui non conosci l'origine o che ti sembrano sospetti. Spesso portano a siti web malevoli, con l'intento di rubare le tue informazioni personali.

Come posso proteggere la mia privacy?

Controlla le autorizzazioni delle applicazioni che installi sul tuo dispositivo, soprattutto quelle gratuite. A volte, per fretta o disattenzione, si tende a dare troppi permessi, come ad esempio l'uso del GPS, della videocamera o del microfono, anche ad applicazioni che in realtà non ne hanno bisogno.

In generale, come buona pratica, ricorda che meno informazioni lasci, meno opportunità offri agli aggressori di attaccarti o di usare i tuoi dati per altri scopi.

Steve Dickenmann
Collaboratore tecnico, Servizio informatica forense
SUPSI

11 Standard e linee guida di riferimento

I settori della sicurezza informatica e delle investigazioni digitali fanno parte di contesti in continua evoluzione, sia da un punto di vista tecnico-scientifico sia regolatorio.

E proprio da quest'ultimo punto di vista ci sono delle normative consolidate e validate a livello internazionale, da conoscere anche a titolo informativo, per acquisire un buon grado di consapevolezza e responsabilità nell'uso delle tecnologie digitali.

In particolare, si segnalano le seguenti fonti ufficiali per il contesto specifico:

- **NIST SP 800-61 Rev.2: Computer Security Incident Handling Guide**

Questa pubblicazione fornisce le linee guida utili per la gestione degli incidenti informatici, in particolare, per analizzare i dati relativi agli incidenti subìti, con lo scopo di determinare la risposta più appropriata e proporzionata a ciascun tipo di incidente (rischio).

Link: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

- **ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection – Information security management systems – Requirements**

Questa norma fornisce i requisiti per un sistema di gestione della sicurezza delle informazioni (ISMS). Il loro utilizzo consente alle organizzazioni di qualsiasi tipo di gestire la sicurezza di beni, come informazioni finanziarie, proprietà intellettuale, dettagli sui dipendenti o informazioni affidate da terzi.

Link: https://www.iso.org/isoiec-27001-information-security.html

- **ISO 22329:2021: Security and resilience – Emergency management – Guidelines for the use of social media in emergencies**

Questa norma propone indicazioni sull'uso dei social media nella gestione delle emergenze. Essa fornisce indicazioni su come le organizzazioni e il pubblico possono utilizzare e interagire attraverso i social media, prima, durante e dopo un incidente. Questo documento è applicabile alle organizzazioni governative e non governative coinvolte nella gestione delle emergenze e nella comunicazione delle crisi.

Link: https://www.iso.org/standard/50066.html

- **ISO/IEC 27035-1:2023: Information technology – Security techniques – Information security incident management – Part 1: Principles and process**

Questa norma presenta i concetti e le basi della gestione degli incidenti di sicurezza delle informazioni, combinandoli con i principi relazionati alle fasi di rilevazione, segnalazione, valutazione e risposta degli incidenti.

Link: https://www.iso.org/standard/78973.html

- **ISO/IEC 27035-2:2023: Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response**

Questa norma fornisce le linee guida per pianificare e preparare la risposta agli incidenti informatici. Le linee guida si basano sulla fase "Pianificazione e preparazione" e sulla fase "Lezioni apprese" del modello "Fasi di gestione degli incidenti di sicurezza delle informazioni" presentato nella ISO/IEC 27035-1 di cui sopra.

Link: https://www.iso.org/standard/78974.html

- **ISO/IEC 27037:2012: Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence**

Questa norma fornisce le linee guida per le attività specifiche di gestione delle prove digitali, utili in fase preventiva e post-incidente, come per esempio per l'identificazione, la raccolta, l'acquisizione e la conservazione di prove digitali che possono avere valore probatorio.

Link: https://www.iso.org/standard/44381.html

- **ISO/IEC 42001: Information technology – Artificial intelligence – Management system**

Questa norma fornisce line guida per progettare, implementare, mantenere e migliorare continuamente un sistema di gestione dell'Intelligenza Artificiale (AIMS) all'interno delle organizzazioni. È progettato per le entità che forniscono o utilizzano prodotti o servizi basati sull'intelligenza artificiale, garantendo lo sviluppo e l'uso responsabile dei sistemi di intelligenza artificiale.

Link: https://www.iso.org/standard/81230.html

Tutte le norme ISO elencate sono disponibili in lingua inglese, quale lingua ufficiale di riferimento.

12 Per saperne di più

Per avere maggiori informazioni potete visitare i seguenti siti web:

- Ufficio federale della cibersicurezza

https://www.ncsc.admin.ch/ncsc/it/home.html

- Ticino Cyber Sicuro

https://www4.ti.ch/di/cybersicuro/home

- Polizia cantonale del Canton Ticino

https://www4.ti.ch/di/pol-new/home

- Servizio informatica forense (SIF), Dipartimento tecnologie innovative, Scuola universitaria professionale della Svizzera italiana SUPSI

https://www.supsi.ch/it/sif

13 Glossario

Account: un account in informatica è come un profilo personale che ti dà accesso a specifiche funzioni, strumenti e contenuti su un sistema o un sito web. È come il tuo spazio personale dove puoi personalizzare le impostazioni e i contenuti, offrendoti una certa privacy poiché le tue attività sono separate da quelle degli altri utenti.

Antivirus: un antivirus è un programma finalizzato a prevenire, rilevare ed eventualmente rendere inoffensivi codici dannosi e programmi malevoli.

Backdoor: una backdoor (dal termine inglese per porta di servizio) è un metodo, spesso segreto, per aggirare la normale autenticazione in un prodotto o un sistema informatico.

Backup: con backup si indica un processo di messa in sicurezza delle informazioni di un sistema informatico attraverso la creazione di una o più copie di riserva dei dati, da utilizzare come recupero dei dati stessi in caso di eventi malevoli accidentali o intenzionali, o semplice manutenzione del sistema.

Cifratura: la cifratura è un processo che trasforma le informazioni leggibili in un formato che non può essere facilmente compreso. Questo viene fatto per proteggere le informazioni sensibili e garantirne la riservatezza. Le informazioni cifrate possono essere lette solo da persone che hanno la chiave appropriata per decifrarle.

Cloud: in questo libro, il termine è usato come riferimento ad uno spazio di archiviazione presente in Internet, come ad esempio Microsoft OneDrive o Google Drive.

Criptovaluta: una criptovaluta o criptomoneta (in inglese *cryptocurrency*) è una valuta digitale ideata per fungere da mezzo di scambio mediante una rete informatica che non è regolata né mantenuta da nessuna autorità centrale, come un governo o una banca. Tra le criptovalute più famose ci sono il Bitcoin ed Ether.

Crittografia: la crittografia (o criptografia) è la branca della crittologia che tratta delle "scritture nascoste", ovvero dei metodi per rendere un messaggio non comprensibile a persone non autorizzate a leggerlo, garantendo così, in chiave moderna, il requisito di confidenzialità o riservatezza tipico della sicurezza informatica.

Deep Web: il Deep Web è la parte di Internet che non viene indicizzata dai motori di ricerca, come Google o Bing. Questo significa che non puoi trovare queste pagine semplicemente cercandole su Google.

Dark Web: Il Dark Web è la parte oscura di Internet che non è indicizzata da motori di ricerca. Le darknet che costituiscono il dark web includono piccole e grandi reti, come ad esempio Tor oppure Freenet, in cui operano organizzazioni pubbliche e singoli individui. Si stima che il 95% dell'attività svolta nel Dark Web sia di natura illegale e questo crea spesso fraintendimenti fra Dark Web e Deep Web, il primo drasticamente meno esteso rispetto al secondo.

Dispositivo USB: Un dispositivo USB è un dispositivo periferico, che si collega a una porta USB di un computer o di altri dispositivi elettronici, per trasferire dati o fornire alimentazione. I dispositivi USB possono variare ampiamente in funzione e forma, includendo

chiavette USB, mouse, tastiere, stampanti, dischi esterni, fotocamere digitali e molti altri dispositivi elettronici. La tecnologia USB consente il collegamento plug-and-play, il che significa che i dispositivi possono essere collegati o scollegati mentre il computer è acceso senza la necessità di riavviare il sistema.

Dominio: un dominio Internet è un nome unico e distintivo a livello globale per un settore specifico di Internet, come ad esempio un sito web. Per fare un esempio, un dominio è come l'indirizzo di casa del tuo sito web su Internet. È un modo semplice per trovare e accedere ai suoi contenuti online.

Estensione di un file: l'estensione di un file, in ambito informatico, è un suffisso, ovvero una breve sequenza di caratteri costituiti da lettere dell'alfabeto e da numeri (tipicamente tre), posto alla fine del nome di un file e separato dalla parte precedente con un punto, attraverso il quale il sistema operativo riesce a distinguerne il tipo di contenuto (testo, musica, immagine, video, ecc.) e il formato utilizzato, per poi aprirlo, di conseguenza, con la corrispondente applicazione. Ad esempio, in un file chiamato "documento.docx", ".docx" è l'estensione che indica che probabilmente il file è un documento di Microsoft Word.

File eseguibile: un file eseguibile (o semplicemente un eseguibile), in informatica, indica un file che contiene un programma eseguibile per un computer, ovvero un programma scritto in "linguaggio macchina", direttamente eseguibile dal processore. Si distingue da un file sorgente, che contiene un programma scritto in un linguaggio di programmazione ad alto livello, il quale può essere eseguito solo utilizzando un interprete o trasformandolo prima in eseguibile, tramite un compilatore, o con una combinazione di strumenti.

Firewall: nell'informatica, nell'ambito delle reti di computer, un firewall è un componente hardware e/o software di difesa perimetrale di una rete, che protegge il computer da malware o altri pericoli di Internet.

Hardware: l'hardware (abbreviato HW) è l'insieme di tutte le parti tangibili elettroniche, elettriche, meccaniche, magnetiche e ottiche che consentono il funzionamento di un computer.

Link: un link è un collegamento ipertestuale, che permette di passare da una pagina web all'altra senza dover ricordare gli indirizzi IP dei server web.

Malware: malware (abbreviazione dell'inglese *malicious software*, lett. "software malevolo"), nella sicurezza informatica, indica un qualsiasi programma informatico usato per disturbare le operazioni svolte da un utente di un computer.

Microsoft Defender: Microsoft Defender è un'applicazione di sicurezza inclusa nell'abbonamento di Microsoft 365 Family o Personal. Tra i suoi servizi vi sono quello di antimalware, con scansioni dei file e applicazioni scaricate, e la protezione Web durante la navigazione che controlla che i link ai siti web non siano dannosi.

Phishing: il phishing è un tipo di truffa effettuata su Internet attraverso la quale, un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari, codici di accesso oppure a eseguire azioni dannose, fingendosi un ente affidabile in una comunicazione digitale.

Ransomware: un ransomware è un tipo di malware che limita l'accesso del dispositivo che infetta, richiedendo un riscatto (*ransom* in inglese) da pagare per rimuovere la limitazione. Ad esempio, alcune forme di ransomware bloccano il sistema e intimano all'utente di pagare, solitamente in criptovalute, per sbloccare il sistema. Altri invece, cifrano i file dell'utente chiedendo di pagare per riportare i file cifrati in chiaro.

Server: un server, in informatica e telecomunicazioni, è un dispositivo fisico o un sistema informatico di elaborazione e gestione del traffico di informazioni. Un server fornisce un qualunque tipo di servizio ad altre componenti (tipicamente chiamate *client*, in italiano clienti), che ne fanno richiesta attraverso una rete di computer.

Sistema operativo: un sistema operativo è un insieme di software che fornisce all'utente una serie di comandi e servizi per usufruire al meglio della potenza di calcolo di un qualsivoglia elaboratore elettronico.

Spyware: uno spyware, in informatica, è un tipo di programma che raccoglie informazioni riguardanti l'attività online di un utente senza il suo consenso.

Tooltip: un tooltip è un piccolo riquadro che compare quando la freccia del mouse si trova su un link e rimane immobile su di esso per alcuni secondi, e visualizza l'indirizzo del link stesso.

Upload: l'upload, anche noto come caricamento, in informatica, è il processo di invio o trasmissione di un file (o più genericamente di un flusso finito di dati o informazioni) da un client ad un sistema remoto (denominato server), attraverso una rete informatica. L'azione inversa è chiamata download.

URL: *Uniform Resource Locator*, anche noto con la sigla URL, è una sequenza di caratteri che identifica univocamente l'indirizzo di una risorsa su una rete di computer, come ad esempio un documento, un'immagine, un video, tipicamente presente su un server e resa accessibile a un client. È perlopiù utilizzato per indicare risorse web ad esempio https://www.google.com.

VPN: una rete privata virtuale (in inglese *virtual private network*, in sigla VPN) è una rete privata, instaurata come connessione tra soggetti. Le VPN possono garantire diversi tipi di protezione dei dati, tra cui confidenzialità, integrità e autenticazione.

ZIP (formato di file): ZIP è un formato di file per la compressione dati senza perdita. Il formato prevede l'utilizzo di diversi algoritmi di compressione dei dati. Oltre a PKZIP, esistono diversi software proprietari e liberi che supportano il formato ZIP, tra cui WinZip e 7-Zip.

Appunti