

Manifesto per l'informazione e la comunicazione responsabile degli incidenti di Cybersicurezza

Perché questo manifesto.

In Italia esistono regole precise su come le organizzazioni devono notificare un incidente informatico (le linee guida ACN per la notifica al CSIRT Italia, gli obblighi GDPR verso il Garante per la protezione dei dati personali), ma non ci sono guide specifiche circa l'applicazione della deontologia professionale giornalistica alle comunicazioni di incidenti di cybersicurezza.

Il Manifesto per l'informazione e la comunicazione responsabile degli incidenti di Cybersicurezza nasce grazie alla collaborazione tra Ordine dei Giornalisti regionale dell'Umbria e Regione Umbria (CSIRT), con l'intento di fornire a chi fa informazione un quadro di riferimento condiviso per raccontare gli incidenti cyber in modo che il diritto di cronaca e il diritto della cittadinanza a essere informato non si traducano, involontariamente, in un danno aggiuntivo per le vittime, per le indagini in corso o per la sicurezza collettiva.

15 principi operativi

1 Verificare prima di pubblicare, sempre.

Prima di diffondere una notizia su un attacco informatico, verifica sempre le fonti (privilegiando quelle ufficiali e primarie, quali per esempio CSIRT regionale, ACN, Agid o Polizia Postale), i fatti, la data e gli impatti dell'incidente, distinguendo informazioni confermate da ipotesi. La fretta può amplificare voci, attribuzioni errate o informazioni utili agli attaccanti.

Evita testi sensazionalistici non verificati come per esempio “Gli hacker hanno rubato tutti i dati dell'azienda”, se l'entità della compromissione non è ancora stata accertata.

2 Aggiornare e correggere quando emergono nuovi elementi.

Una comunicazione responsabile non si ferma alla prima versione dei fatti. Un incidente informatico è per sua natura evolutivo, ed è normale che con l'avanzare delle indagini e delle verifiche tecniche ci siano degli aggiornamenti e delle nuove informazioni che devono essere aggiornate o altre date in precedenza che devono invece essere corrette.

Per esempio, qualora sia stato smentito un Data Breach che era stato annunciato, è necessario riportare un aggiornamento che sottolinei per esempio “le verifiche hanno escluso, al momento, l'esfiltrazione di dati personali. La notizia precedente viene pertanto corretta”.

3 Proteggere le vittime.

Racconta l'incidente informatico senza esporre inutilmente persone, aziende o soggetti coinvolti a ulteriori rischi, evitando di pubblicare dati personali, credenziali, dettagli sensibili o informazioni che possano facilitarne l'identificazione o una nuova compromissione.

Evita, per esempio, di pubblicare screenshot di database rubati contenenti dati personali, anche se pensati per dare “prova” dell'attacco.

4 Non fare da cassa di risonanza agli attaccanti.

Informa sull'attacco senza amplificare la propaganda, le minacce o le richieste degli aggressori, evitando di trasformare la comunicazione in uno strumento di pressione sulle vittime.

Evita, per esempio, di pubblicare integralmente il messaggio degli attaccanti, i loro slogan o i link ai dati sottratti, contribuendo a dare voce ai cyber criminali.

5 Non pubblicare dettagli tecnici che facilitano nuovi attacchi.

Concorda con CSIRT regionale, Polizia Postale e organizzazioni coinvolte i dettagli tecnici da poter divulgare, evitando di diffondere informazioni operative che possano essere riutilizzate per colpire altre vittime, come per esempio specificare la versione del software vulnerabile, indirizzi di rete o procedure di accesso. Spiega in termini comprensibili (con l'aiuto dei tecnici che se ne stanno occupando) quale vulnerabilità è stata sfruttata e quali conseguenze ha avuto, senza fornire istruzioni per replicare l'attacco.

6 Usare un linguaggio corretto, non sensazionalistico.

Racconta l'attacco con parole precise e proporzionate, evitando termini come “catastrofe”, “cyber guerra” o “hacker scatenati” quando non descrivono correttamente i fatti.

Il linguaggio va adattato al mezzo: sui social network occorre essere sintetici ma accurati, mentre articoli, comunicati e approfondimenti possono fornire contesto, fonti e distinguere fatti da ipotesi. Evita anche titolazioni acchiappa clic quali “ATTACCO SHOCK! L'azienda XXXX è sotto assedio degli hacker!”.

7 Contestualizzare l'impatto reale, senza esagerare né minimizzare.

Comunicare un attacco significa informare sui possibili impatti, cercando di comprendere quelli reali e probabili grazie al supporto di CSIRT e forze dell'ordine.

Un'interruzione temporanea di un servizio, una violazione di dati personali o una compromissione di infrastrutture critiche possono avere conseguenze molto diverse e ripercussioni sul comportamento della cittadinanza di diversa entità, da non sottovalutare. Per esempio, scrivere che non sarà più possibile effettuare visite mediche in un ospedale a seguito di un cyber attacco può spingere i cittadini a contattare inutilmente le strutture sanitarie, cancellare o rinviare prestazioni, sovraccaricare i centralini e i servizi di emergenza e, nei casi più gravi, compromettere l'accesso alle cure di chi ne ha realmente bisogno.

8 Dare voce a chi è stato colpito con tempi ragionevoli.

Informare in modo responsabile significa anche ascoltare le persone e le organizzazioni coinvolte, lasciando loro il tempo necessario per verificare i fatti, valutare l'impatto e comunicare informazioni affidabili. Nelle prime ore successive a un incidente, le organizzazioni sono assorbite dalle procedure urgenti di contenimento dell'incidente, ripristino dei servizi e dialogo con le autorità. La ricerca della notizia non deve, pertanto, trasformarsi in una pressione ulteriore su chi sta gestendo l'emergenza e anche una mancata risposta può essere accolta nei primi momenti come segno di attenzione finalizzato ad affrontare al meglio la crisi dovuta all'incidente.

È possibile contattare l'organizzazione colpita, raccogliere la sua posizione senza pretendere di avere informazioni che non sono state ancora concordate per esempio con le forze dell'ordine.

9 Sostenere la cultura della prevenzione di Cybersicurezza.

Il ruolo dei giornalisti non è limitato al solo racconto degli incidenti informatici, ma può contribuire a far comprendere ai cittadini come riconoscere e prevenire i rischi informatici.

Può essere utile valorizzare e, quando possibile, coordinarsi con le campagne istituzionali già esistenti, come quelle promosse dalla Polizia Postale, per rafforzare messaggi e comportamenti condivisi.

10 Evitare di fornire elementi che possano ostacolare le indagini.

La comunicazione di un attacco informatico deve tenere conto delle attività investigative in corso e deve, pertanto, evitare la divulgazione di informazioni che possano compromettere la raccolta delle prove, allertare gli autori dell'attacco o influenzare le testimonianze. È importante distinguere tra il diritto di informare e la necessità di non rendere pubblici dettagli che devono rimanere riservati alle autorità e ai soggetti coinvolti.

Per una corretta informazione, è sempre consigliabile rapportarsi con le autorità che stanno svolgendo indagini per evitare di anticipare elementi investigativi non ancora confermati o che forniscono agli attaccanti informazioni utili per eludere le verifiche.

11 Verificare tutto ciò che è stato prodotto dall'IA.

L'intelligenza artificiale può aiutare a raccogliere le fonti, a sintetizzare e a scrivere bozze di contenuti rapidamente, ma occorre fare una grande attenzione, visto che può generare informazioni inesatte, attribuzioni errate o riportare fonti e dettagli non verificati. Ogni contenuto prodotto dall'IA deve quindi essere controllato attraverso fonti affidabili prima della pubblicazione, soprattutto quando riguarda responsabilità, dati personali o dettagli tecnici di un attacco.

I punti che seguono sono rivolti agli uffici stampa e ai responsabili della comunicazione delle organizzazioni potenzialmente colpite da un incidente, con l'obiettivo di facilitare un dialogo efficace e tempestivo con i giornalisti.

12 Stabilire un flusso e un piano della comunicazione dell'incidente.

Gli uffici stampa dovrebbero pianificare in anticipo come gestire la comunicazione in caso di incidente cyber, definendo chi comunica, attraverso quali canali e con quali tempi.

Un piano condiviso permette di fornire ai giornalisti riferimenti chiari fin dalle prime ore, evitando dichiarazioni contraddittorie o rilasciate da fonti non autorizzate, che rischiano di generare confusione anche nella cronaca dei fatti.

È possibile ispirarsi a diverse prassi - anche internazionali - che consigliano la definizione di un piano della comunicazione di crisi, con un'unità di crisi, ruoli e responsabilità, un portavoce unico, i flussi informativi e i canali da utilizzare verso i media.

13 Preparare alcuni messaggi iniziali.

In caso di attacco cyber, è utile che l'ufficio stampa predisponga in anticipo alcune dichiarazioni essenziali da poter rilasciare rapidamente ai giornalisti, insieme a un calendario di aggiornamenti periodici concordato tra vertice aziendale, struttura informatica e funzioni competenti. Avere un messaggio iniziale pronto, anche minimo, aiuta a soddisfare la legittima richiesta di informazione della stampa senza dover rincorrere le notizie che circolano nel frattempo su altri canali.

14 Individuare canali alternativi di comunicazione.

Nella gestione di un attacco è opportuno considerare che i canali ordinari (sito, email istituzionale, centralino) potrebbero non essere disponibili. È quindi consigliabile che l'ufficio stampa individui in anticipo, all'interno del piano di gestione della crisi cyber, strumenti alternativi per restare raggiungibile dai giornalisti e continuare a garantire un flusso informativo minimo anche quando l'infrastruttura abituale è compromessa.

15 Programmare simulazioni pratiche.

Per verificare che il piano di gestione della crisi cyber sia realmente efficace, è opportuno che l'ufficio stampa partecipi a simulazioni ed esercitazioni periodiche insieme alle altre funzioni coinvolte (struttura informatica, vertice, legale). Provare in anticipo come si gestirebbe una richiesta urgente di informazioni da parte dei giornalisti - comprese le domande più scomode - permette di individuare per tempo eventuali falle nel piano di comunicazione e di arrivare preparati al momento in cui l'incidente si verifica davvero.

GLOSSARIO

ACN (Agenzia per la Cybersicurezza Nazionale): autorità nazionale italiana preposta alla tutela della sicurezza cibernetica e della resilienza digitale del Paese.

CSIRT (Computer Security Incident Response Team): struttura che monitora gli eventi informatici, riceve le notifiche di incidente, eroga supporto alle organizzazioni oggetto di cyber attacco e coordina la risposta operativa a livello nazionale o regionale.

Baiting tecnica di adescamento realizzata tramite chiavette USB o altri dispositivi USB lasciati incustoditi al fine di indurre la vittima a compiere un'azione che va a compromettere il sistema.

Data Breach incidente di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o trattati dall'organizzazione vittima di attacco.

DDoS (Distributed Denial of Service): attacco informatico realizzato attraverso l'invio massivo di richieste fittizie verso un server o una rete, al fine di sovraccaricarli e renderli temporaneamente inaccessibili agli utenti legittimi (di norma senza comportare sottrazione di dati).

Dark Web porzione di Internet non indicizzata dai comuni motori di ricerca e accessibile soltanto tramite strumenti specifici, spesso utilizzata da organizzazioni criminali per scambiare informazioni e merci illecite o pubblicare dati sottratti.

Exploit programma, codice o sequenza di comandi sviluppato per sfruttare una specifica vulnerabilità di un sistema informatico al fine di acquisirne il controllo o causare malfunzionamenti.

Malware termine generale che include virus, ransomware e spyware creati per danneggiare, bloccare o rubare dati dal sistema informatico di una organizzazione.

Path indirizzo che indica dove si trova un file o una risorsa all'interno di cartelle o sottocartelle di un sistema.

Phishing tecnica di ingegneria sociale con la quale malintenzionati inviano comunicazioni ingannevoli (e-mail, SMS, messaggi) per indurre i destinatari a rivelare informazioni confidenziali (come password o credenziali bancarie) o a scaricare software malevoli.

Spear Phishing forma mirata di phishing in cui un attaccante invia messaggi fraudolenti personalizzati a una specifica persona o a una organizzazione, con l'obiettivo di indurla a rivelare informazioni riservate, fare clic su un link, aprire un allegato dannoso o compiere un'altra azione.

Vishing forma di phishing effettuata tramite chiamate vocali o comunicazioni telefoniche, in cui l'attaccante si finge una persona o un'organizzazione affidabile per indurre la vittima a fornire informazioni riservate, come password, codici di autenticazione o dati bancari, oppure a compiere determinate azioni.

Whaling forma di phishing mirato rivolta a persone che ricoprono ruoli di particolare rilievo all'interno di un'organizzazione, come dirigenti, amministratori delegati o responsabili finanziari.

Ransomware tipologia di malware che cifra i file o blocca l'accesso ai sistemi della persona o organizzazione oggetto dell'attacco informatico, rendendoli inutilizzabili fino al pagamento di un riscatto (ransom).

SOC (Security Operations Center): team centralizzato dedicato alla sicurezza informatica di un'organizzazione, incaricato di monitorare, rilevare, analizzare e gestire le minacce e gli incidenti di sicurezza.

Social Engineering (ingegneria sociale): tecnica di manipolazione psicologica che sfrutta le vulnerabilità umane per ingannare le persone e portarle a compiere azioni. L'obiettivo del social engineering è spesso quello di spingere le vittime a rivelare dati sensibili, password, o compiere azioni che compromettono la sicurezza informatica.

Threat Actor individuo, gruppo criminale, collettivo di persone che progettano ed eseguono attività cibernetiche malevole.

Vulnerabilità informatica debolezza o difetto nella progettazione, configurazione o gestione di un sistema informatico, che può essere sfruttata per violarne i requisiti di sicurezza.

CHECKLIST RAPIDA PRIMA DI PUBBLICARE

Per giornalisti

- Ho verificato la notizia con fonti ufficiali e primarie (CSIRT regionale, ACN, Agid, Polizia Postale)?
- Ho almeno due fonti indipendenti o una fonte ufficiale che parla dell'incidente cyber?
- Ho distinto chiaramente ciò che è confermato da ciò che è ancora ipotesi?
- Se ho usato l'IA per raccogliere fonti o scrivere una bozza, ho controllato ogni informazione (fatti, attribuzioni, dettagli tecnici) su fonti affidabili prima di pubblicare?
- Ho eliminato dal pezzo dati personali, siti dove sono stati esfiltrati dati o pubblicate immagini non autorizzate, dettagli che potrebbero facilitare l'identificazione delle vittime o una nuova compromissione?
- Ho verificato con la redazione la pubblicazione dell'immagine associata affinché non sia, per esempio, uno screenshot di database rubati o altro materiale "prova" che contiene dati personali?
- Ho verificato con CSIRT, Polizia Postale o con l'organizzazione coinvolta quali dettagli tecnici (versioni software, indirizzi di rete, procedure di accesso) è opportuno divulgare?
- Il pezzo spiega la vulnerabilità senza fornire, di fatto, istruzioni per replicare l'attacco?
- Ho previsto una modalità di aggiornamento della notizia, qualora emergano nuovi elementi rispetto a un mio articolo precedente?
- Ho inserito nell'articolo tutti gli aggiornamenti e le correzioni che sono state fornite?
- Il linguaggio usato (titolo compreso) è proporzionato ai fatti, senza termini come "catastrofe", "cyber guerra" o titoli acchiappa-clic?
- Ho valutato l'impatto reale dell'incidente cyber (per esempio su servizi essenziali legati all'ambito sanitario) senza esagerare né minimizzare le conseguenze per la cittadinanza?
- Ho lasciato all'organizzazione colpita un tempo ragionevole per rispondere, evitando di trasformare la richiesta di notizia in una pressione ulteriore?
- Ho verificato che non ci siano nel pezzo particolari che potrebbero ostacolare le indagini in corso (prove, testimonianze, dettagli riservati alle autorità)?

Per uffici stampa dell'organizzazione vittima di attacco

CHECKLIST PER GLI UFFICI STAMPA - GESTIONE DELLA COMUNICAZIONE DI CRISI

Azioni preventive

- Esiste un piano di comunicazione di crisi cyber, con unità di crisi, ruoli, responsabilità e un portavoce unico definiti in anticipo?
- Sono stati preparati messaggi iniziali essenziali, pronti da rilasciare rapidamente ai giornalisti in caso di incidente?
- È stato definito un calendario di aggiornamenti periodici, concordato tra vertice, struttura informatica, comunicazione e funzioni competenti?
- Sono stati individuati canali di comunicazione alternativi, nel caso in cui sito, email istituzionale o centralino risultino compromessi o non disponibili?
- Sono state programmate simulazioni ed esercitazioni periodiche, comprese le domande più scomode dei giornalisti, per testare l'efficacia del piano?

Gestione dell'incidente

- Il portavoce designato è l'unico a rilasciare dichiarazioni ufficiali, per evitare messaggi contraddittori?
- I giornalisti ricevono riferimenti chiari fin dalle prime ore (chi contattare, con quali tempi)?
- Le informazioni diffuse sono state concordate con CSIRT regionale e/o Polizia Postale, evitando dettagli tecnici che potrebbero facilitare nuovi attacchi?
- Se non è ancora possibile confermare l'entità del danno, è stato comunicato con chiarezza cosa è confermato e cosa è ancora in verifica?

Aggiornamento e chiusura

- Sono stati comunicati gli aggiornamenti man mano che le verifiche tecniche e le indagini procedono?
- Se una notizia precedente è stata smentita o ridimensionata, è stata pubblicata una correzione esplicita?
- È stato organizzato un momento interno di retrospettiva sull'efficacia della gestione della comunicazione, per migliorare il piano in vista di futuri incidenti?

DOCUMENTI PRINCIPALI DI RIFERIMENTO PER LA COMUNICAZIONE DEGLI INCIDENTI

NIST SP 800-61 Rev. 3 - Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile

Link: <https://csrc.nist.gov/pubs/sp/800/61/r3/final>

Raccomandazioni contenute nel documento:

- predisporre un Communication Plan prima degli incidenti;
- identificare chi comunica e con quale autorità;
- definire stakeholder interni ed esterni;
- utilizzare messaggi approvati;
- evitare informazioni non verificate;
- mantenere aggiornamenti periodici;
- documentare tutte le comunicazioni effettuate.

ENISA - BEST PRACTICES FOR CYBER CRISIS MANAGEMENT

Link: <https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management>

ISO/IEC 27035-1:2023 INFORMATION TECHNOLOGY - INFORMATION SECURITY INCIDENT MANAGEMENT PART 1: PRINCIPLES AND PROCESS

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

A FRAMEWORK FOR EFFECTIVE CORPORATE COMMUNICATION AFTER CYBER SECURITY INCIDENTS

Link: <https://arxiv.org/abs/2009.09210>

CRISIS COMMUNICATION IN THE FACE OF DATA BREACHES

Link: <https://arxiv.org/abs/2406.01744>

DIRETTIVA NIS2

Link: <https://eur-lex.europa.eu/eli/dir/2022/2555/>

FONTI ITALIANE CITATE NEL MANIFESTO

ACN <https://www.acn.gov.it/portale/home>

CSIRT Italia <https://www.acn.gov.it/portale/csirt-italia>

CSIRT Regione Umbria <https://csirt.regione.umbria.it/>

CERT_AGID <https://cert-agid.gov.it/>

Polizia Postale <https://www.commissariatodips.it/index.html>

Associazione Clusit <https://clusit.it/>

