Il silenzio di OPL durante l’attacco degli hacker

L’Ordine degli Psicologi della Lombardia è stato vittima di un attacco hacker.

Il data breach pare essersi svolto il 03 ottobre scorso.
Nei giorni successivi si sono attivate immediatamente tutte le procedure necessarie per monitorare, comprendere e gestire la situazione.
In poco tempo è stato ripristinato l’accesso alla rete e a tutti gli archivi, limitando di pochissimo le complessità.

Il 10 ottobre, una settimana dopo, il collettivo NoEscape rivendica l’attacco pubblicando, sul suo sito, la notizia di aver bucato gli archivi di OPL. Siamo difronte ad un attacco ransomware. Si tratta di una tipologia di malware che blocca l’accesso a un computer cifrando i dati in esso contenuti, con l’obiettivo di ottenere un riscatto dalla vittima.
Nel comunicato, **gli hacker dicono di aver prelevato circa 7gb di dati**, tra i quali documenti di identità, accordi e contratti, documenti finanziari, report e documenti vari, **e ne minacciano il rilascio entro circa 6 giorni.**

Fino a qui, nessuna comunicazione viene data agli iscritti e nessuna news viene pubblicata nella sezione notizie del sito di OPL.
Solo undici giorni dopo, durante il Consiglio del 14 ottobre riceviamo notizia sommaria del data breach, attraverso una nota del DPO (Data Protection Officer) dell’Ordine, che la presidente Parolin legge durante la riunione senza tuttavia aggiungere nulla.

Il 18 ottobre il collettivo di hacker rende disponibile l’elenco dei file e delle cartelle in possesso, rimandandone la pubblicazione tra altri 6 giorni.

Ancora nessuna comunicazione presente sul sito istituzionale dell'Ordine, ma incominciano a girare sui social alcuni articoli blog di esperti di sicurezza informatica come Edoardo Limone (**https://shorturl.at/nsFUY**) o Chiara Nardini (**https://shorturl.at/cCNY2**) che seguono i fatti e provano a darne spiegazione dal punto di vista tecnico.

Il 19 ottobre, verificate le caratteristiche dell'attacco e della possibile fuga di dati, l'Ordine presenta la notifica della violazione al Garante per la protezione dei dati personali, con un ritardo di quasi due settimane da quanto richiesto dalla normativa di riferimento, la quale dice che *"Le notifiche al Garante devono essere effettuate entro il termine delle 72 ore o in caso di ritardo accompagnate da motivi"*. Possiamo immaginare che il motivo del ritardo fossero proprio le operazioni di verifica.

Passati i sei giorni di attesa, al 24 ottobre, il sito di NoEscape è indisponibile, nessun dato risulta pubblicato nel web tradizionale e i server di OPL continuano a funzionare regolarmente.

MA LA COMUNICAZIONE AGLI ISCRITTI?
In tutti questi 20 giorni Opl ha evitato di raccontare ufficialmente sui canali istituzionali quanto stesse accadendo.
Una scelta che non condividiamo, proprio perché, al di là della reale gravità del danno, gli iscritti vanno informati di tutto quello che è appartenente alla vita ordinistica in modo trasparente.

La nostra legge istitutiva (lg 56/89) ci ricorda che l'albo è costituito dagli psicologi e dalle psicologhe ad esso iscritti e che il consiglio eletto ne esercita le funzioni attribuite. Questo ci deve ricordare che siamo lì per esercitare un ruolo istituzionale, che siamo stati eletti e che le scelte, richiamabili tra le funzioni, vanno comunicate e condivise con gli iscritti all'Albo.

È una regola semplice: eserciti la funzione istituzionale e comunichi agli iscritti.

Ma **l'unica comunicazione di OPL viene pubblicata il 21 ottobre e non si tratta di una comunicazione spontanea, bensì di un comunicato stampa in risposta ad un articolo pubblicato su Open (https://shorturl.at/gpX04) a dimostrazione che l'interesse non fosse di informare i colleghi iscritti all'Ordine, ma di rispondere al giornale.**

Comunicato nel quale la Presidente ci rassicura che l'attacco informatico è stato ampiamente scongiurato, salvo poi inviarci una nuova comunicazione per dirci che nuovamente il sito ha subito un attacco informatico il 24 e 25 ottobre (**https://shorturl.at/bnwMP**). Cosa che può accadere, ma il problema vero è l'assenza di una comunicazione trasparente ai colleghi.
Nessuna rassicurazione, nessuna strategia, nessuna parola per orientare i colleghi, nessuna condivisione in consiglio, mentre sui social e nei canali privati giravano domande e preoccupazioni.

Nei primi 20 giorni sono state inviate 5 newsletter e aggiornate 6 nuove news sul sito, ma di data breach neanche l'ombra e se non racconti fin da subito cosa sta accadendo, dai spazio a tutto il resto: notizie distorte, passaparola, incomprensioni, ecc.

Si poteva mandare una Newsletter, fare un comunicato video da divulgare sui canali social, chiedere la pubblicazione di un comunicato stampa, avvisare una testata giornalistica a taratura nazionale/regionale, postare aggiornamenti su facebook, intervistare un esperto di cybersecurity.

Si poteva fare tanto, dimostrando a chi ci sta attaccando che siamo una comunità ampia e solida, e invece non si è fatto nulla.
In tutto questo, rimane il fatto che **l'Ordine è stato**

politicamente e dialetticamente assente, dimenticandosi che qui in consiglio siamo solo 15 persone, mentre fuori ce ne sono altri 23mila.

Quello che davvero non funziona è questo modo di trattare gli iscritti all'Ordine come sudditi, da imbonire con una serie di informazioni inutili, piuttosto che come fruitori di un servizio pubblico a cui destinare un'informazione utile e trasparente, anche quando si tratta di notizie sgradevoli, che potrebbero mettere in cattiva luce il monarca e i suoi cortigiani.