VADEMECUM SULLA SICUREZZA INFORMATICA NEGLI STUDI LEGALI

A cura dell'Avv.Andrea Lisi
DPO dell'ORDINE DEGLI AVVOCATI DI LECCE

Il presente Vademecum contiene la descrizione delle procedure e misure di sicurezza tecniche e organizzative da adottare all'interno degli Studi legali, alla luce delle disposizioni del Regolamento Europeo n. 679/2016 (General Data Protection Regulation – GDPR), del D.Lgs. n. 196/2003 (Codice in materia di protezione dei dati personali), dei provvedimenti dell'Autorità Garante per la protezione dei dati personali e dell'European Data Protection Board (ex WP 29).

Il Vademecum è a cura dell'Avv. Andrea Lisi, DPO dell'Ordine degli Avvocati di Lecce. Hanno collaborato alla stesura i componenti del Team del DPO:

Avv. Sarah Ungaro

Avv. Carola Caputo

Avv. Mario Montano

Il presente documento è stato espressamente realizzato per l'Ordine degli Avvocati di Lecce.

Lecce, 16 ottobre 2019

Sommario

Premesse

Il principio di *accountability*, introdotto dal GDPR, comporta per qualsiasi organizzazione - compresi gli Studi professionali – una necessaria e approfondita auto-analisi sia della modalità di circolazione (interna ed esterna) dei dati personali (e quindi delle procedure in essere per legittimarne il trattamento), che delle misure di protezione messe in atto. È inoltre necessario monitorare la correttezza delle procedure di trattamento e protezione dei dati personali soprattutto sotto il profilo giuridico, oltre che tecnico-informatico.

Si precisa in proposito che occorre distinguere tra il modello organizzativo di *assessment* per la protezione del dato – da finalizzare attraverso una metodologia di analisi prevalentemente organizzativa e di controllo – e lo sviluppo di politiche di sicurezza informatica a protezione del patrimonio informativo e documentale. In ottica GDPR, queste ultime devono essere soppesate in base ad un'indispensabile analisi preventiva, che tenga conto della tipologia dei dati trattati e dei rischi reali che corrono gli stessi database e archivi.

In particolare, per essere *compliant* rispetto alle norme del GDPR, non sarà più sufficiente adottare un approccio meramente formalistico, che si traduceva sino a oggi, nella maggior parte dei casi, nell'adozione delle misure minime di sicurezza di cui all'Allegato B (ormai abrogato) del D.Lgs. 196/2003, nella redazione di informative e nomine a responsabili e incaricati e nell'acquisizione dei consensi degli interessati, ove necessario.

Nel nuovo scenario normativo infatti, che delinea un approccio di *accountability* (ovvero di "responsabilizzazione"), il Titolare del trattamento deve porre in essere tutte le misure di sicurezza in termini sì tecnologici, ma soprattutto organizzativi, adeguate a dimostrare (e documentare) di aver improntato i trattamenti di dati personali ai principi della privacy *by design* e alla privacy *by default* (a mero titolo esemplificativo: istituendo e alimentando correttamente il Registro dei trattamenti; adottando una procedura per analizzare i rischi di ogni trattamento e quindi decidere se effettuare un Privacy Impact Assessment; verificando che l'archiviazione dei dati personali nelle banche dati degli Studi legali sia strutturata in modo idoneo e permetta anche di poter garantire agli interessati i nuovi diritti riconosciuti agli stessi dal GDPR, etc.).

In particolare, occorre considerare che gli Studi legali detengono e gestiscono un ingente volume di informazioni di natura personale e commerciale relativa non solo ai clienti, ma anche a collaboratori e dipendenti. Ciò rende queste realtà, piccoli o grandi che siano, un potenziale obiettivo dei cybercriminali. Una violazione della sicurezza dei dati può avere degli effetti legali, economici e reputazionali devastanti sia per i clienti, che per gli stessi studi legali. Per questo è fondamentale che i Titolari del trattamento si dotino di misure di sicurezza efficaci, al fine di preservare la riservatezza, l'integrità e la disponibilità dei dati, specie di quelli appartenenti a categorie particolari o relativi a condanne penali o reati (ai sensi degli artt. 9 e 10 del GDPR).

È stato osservato che spesso gli studi legali sono oggetto di cyberattacchi a causa della mancanza di consapevolezza dei rischi da parte degli avvocati o della scarsità di risorse finanziarie adeguate a garantire misure tecnologiche efficaci contro attacchi ai sistemi informativi.

È il caso della violazione di un *account* di posta attraverso la tecnica del *phishing*, a cui può seguire la distribuzione di un *ransomware* (un virus in grado di criptare l'intero *hard disk*, impedendone l'accesso all'utilizzatore fino al pagamento di un riscatto, in genere in *bitcoin*) alle caselle di posta di altri professionisti, sfruttando il meccanismo di fiducia generato da mail inoltrare da Colleghi.

È importante, infine, sottolineare la necessità di un dialogo fra avvocati ed esperti in materia di nuove tecnologie e tutela dei dati personali a garanzia dei propri clienti, proprio come già avviene allorché un avvocato necessiti di competenze specialistiche per comprendere una fattispecie e difendere al meglio il cliente, assolvendo, fra l'altro, ad un preciso dovere deontologico.

Sulla base di quanto detto nelle premesse, si darà conto, di seguito, di alcune regole da seguire come buona prassi per impostare una corretta gestione degli strumenti informatici utilizzati nello svolgimento dell'attività lavorativa, suddivise in tre macro- aree:

- **Tecnologia;**
- **Processi organizzativi;**
- **Formazione del personale**.

Tecnologia

Possedere tecnologie aggiornate ed efficienti è il primo passo per minimizzare gli effetti di un attacco informatico e proteggere i dati personali posseduti. I concetti di seguito descritti, pur non approfondendo i risvolti strettamente tecnici, sono utili al professionista per acquisire gli strumenti necessari al riconoscimento di un rischio, al fine di valutarlo e richiedere, eventualmente, l'assistenza di un esperto IT, interpellandolo correttamente e dunque essendo in grado di seguirlo nell'attività da svolgere.

Mantenere i software aggiornati

Può apparire una banalità, ma non esiste un software che non abbia dei vizi, degli errori nel codice di programmazione (c.d. bug). Sono queste le vulnerabilità che gli hacker sfruttano per introdursi all'interno delle macchine e così sottrarre informazioni, dati personali, attivare la webcam, il microfono, leggere le parole digitate sulla tastiera, tutto all'insaputa dell'utilizzatore.

Azioni da intraprendere:

- Acquistare antivirus di livello e software per filtrare le mail;
- Assicurarsi di aggiornare il sistema operativo (Windows, Mac OS X, Linux), verificando la disponibilità di aggiornamenti o il rilascio di nuove versioni e solo da fonti ufficiali (ad. es. Windows Update). È preferibile impostare l'aggiornamento automatico del suddetto sistema operativo;
- Assicurarsi che gli aggiornamenti del firmware siano effettuati non solo sui PC ma anche sui modem e i router;
- Effettuare la scansione antivirus automatica di tutti gli allegati alle mail, senza lasciare questo compito agli utenti.

Protezione degli *endpoint*

Qualunque dispositivo connesso alla rete dello studio (PC, smartphone, stampante, ecc.) è un *endpoint*. Tramite queste "porte" entrano ed escono i dati dalla rete verso internet: è fondamentale che siano adeguatamente protette e monitorate.

Azioni da intraprendere:

- Implementare protezioni antivirus e firewall che filtrino un certo tipo di traffico di rete al fine di proteggere i sistemi informatici e tenere traccia del traffico.

Utilizzare connessioni internet sicure

Accedere a reti Wi-Fi poco sicure (come quelle di alberghi, bar, ristoranti, aeroporti) significa essere esposti alla probabile intercettazione dei dati personali e/o informazioni sensibili da parte dei cybercriminali.

Qualora i dipendenti o i collaboratori lavorino da remoto (ad esempio a casa o durante una trasferta), devono accertarsi che la connessione utilizzata sia sicura, utilizzando una *virtual private network* (VPN) e non una connessione Wi-Fi pubblica. Una VPN è una connessione cifrata, una sorta di tunnel virtuale all'interno della rete utilizzata e può essere creata con l'utilizzo di semplici *software* o *app*.

Sicurezza del browser e delle e-mail

Le e-mail e la navigazione Internet sono i due principali vettori utilizzati dagli hacker per effettuare un attacco.

Azioni da intraprendere:

- Aggiornare costantemente il browser utilizzato (Chrome, Firefox, Safari, Microsoft Edge o Internet Explorer, ecc.);
- Disabilitare la funzione di auto-completamento/auto-riempimento;
- Disabilitare la connessione a internet di computer o server quando non necessaria;
- Non utilizzare caselle di posta elettronica gratuite. Sono senz'altro da preferire servizi a pagamento generalmente riconosciuti.

Crittografare dati e dispositivi

La crittografia è una tecnica che permette di rendere illeggibili i file a chi non possiede la password o la chiave per sbloccarli. Possono essere criptati sia file contenuti in un dispositivo o hard disk, sia file trasmessi telematicamente (v. la VPN).

Azioni da intraprendere:

- Criptare file contenenti dati personali appartenenti a categorie particolari o relativi a condanne penali o reati;
- Criptare tutti i PC, tablet, smartphone che possono memorizzare o trasmettere dati;
- Cercare di limitare l'accesso ai dati più importanti solo ai collaboratori autorizzati o ai dispositivi necessari.

Cancellazione da remoto

È abbastanza frequente che si verifichi la perdita o la sottrazione di uno smartphone, di un PC o di altro dispositivo. Nel caso in cui il dispositivo non sia crittografato è sempre possibile installare un software in grado di cancellare alcuni o tutti i file da remoto, a patto che il software sia già presente nel dispositivo prima dello smarrimento/sottrazione.

Azioni da intraprendere:

- Installare un software per la cancellazione dei dati da remoto. Il software opererà soltanto se il dispositivo è connesso ad internet.

Cloud Computing

Molto sinteticamente, il cloud computing consiste nell'erogazione di servizi (software, app, storage, e-mail) da parte di un provider a richiesta di un cliente attraverso la rete internet e resi disponibili su risorse server in remoto.

Azioni da intraprendere:

- Assicurarsi che i dati dei clienti siano memorizzati in un luogo soggetto alla medesima giurisdizione alla quale è soggetto il Titolare del trattamento. Questo perché molti Stati consentono a terze parti (soprattutto autorità governative) di controllare i dati degli Studi legali, compromettendo la riservatezza dei loro clienti;
- Assicurarsi che il provider implementi politiche di sicurezza adeguate;
- Verificare se i dati sono memorizzati con sistemi di crittografia;
- Verificare quali siano i sistemi di autenticazione al cloud e se è possibile l'autenticazione a due fattori (es. pin + token);
- Assicurarsi che il provider effettui regolarmente dei back-up e verificare quale sia la politica di conservazione dei dati (c.d. *data retention*).

Gestione del controllo degli accessi

Il controllo degli accessi riguarda il diritto riconosciuto ad alcuni individui di accedere a tutta o parte della rete internet dello Studio legale, ma anche alle risorse e ai file che possono essere gestiti su *storage* condivisi.

Azioni da intraprendere:

- Ridurre al minimo gli *account* amministratore (quelli che hanno accesso completo a tutte le risorse);

- Individuare quali risorse necessitino del livello di autorizzazione più elevato e utilizzare profili amministrativi specifici con privilegi ridotti;
- Restringere l'accesso ai documenti e alle risorse ai soli utenti che ne hanno bisogno per svolgere i propri compiti;
- Bloccare prontamente l'accesso ai collaboratori/dipendenti che non fanno più parte dello Studio, per evitare accessi non autorizzati da remoto;
- Predisporre delle apposite policy o regolamenti sull'utilizzo degli strumenti e delle risorse informatiche dello Studio legale che i collaboratori/dipendenti siano tenuti a rispettare.

Sicurezza dei dispostivi mobili

È indubbio che negli ultimi anni si sia assistito a un incremento notevole dei dispositivi mobili per svolgere le attività professionali, sia personali (c.d. BYOD, *bring your own device*) sia aziendali. Essi, tuttavia, contengono dati personali sia dell'utilizzatore del dispositivo, che relativi alle attività dello studio legale. Pertanto, è consigliabile crittografare il dispositivo mobile in uso e intraprendere ulteriori azioni a tutela della sicurezza dei dati.

Azioni da intraprendere:

- Redigere una policy sull'uso dei BYOD che definisca chiaramente le condizioni e i limiti dell'utilizzo dei dispositivi mobili nell'attività professionale;
- Utilizzare una soluzione MDM (Mobile Device Management) per proteggere i dati dello Studio legale. Se possibile, preferire soluzioni che separino i dati personali dell'utilizzatore del dispositivo da quelli relativi alle attività dello Studio legale;
- Se si utilizza il dispositivo personale (circostanza molto frequente) per l'attività professionale, definire delle impostazioni di sicurezza rigorose per assicurare un ambiente di lavoro sicuro (ad es. una password di accesso robusta, un meccanismo di scadenza della password, blocco dell'accesso al dispositivo trascorso un certo tempo e la crittografia del dispositivo).

Processi organizzativi

La maggior parte dei successi dei cyberattacchi è dovuta a errori umani. Non è possibile prevenire ogni attacco, ma definire dei processi organizzativi è fondamentale per comprendere quali siano le attività, i ruoli e i documenti necessari a uno studio legale al fine di mitigare i rischi di un attacco informatico.

Quelli che seguono sono dei consigli pratici la cui implementazione consente di arginare la gran parte degli attacchi informatici.

Utilizzo di username e password robuste accanto a sistemi di autenticazione a due fattori

- Utilizzare username e password complesse. In particolare, la password dovrà essere composta da un minimo di 8 caratteri contenenti lettere maiuscole, minuscole, cifre e caratteri speciali. Prevedere un sistema che richieda automaticamente agli utenti di cambiare la password almeno una volta ogni tre mesi;
- Utilizzare un sistema di autenticazione a due fattori (es. password + token);
- Assicurarsi che la stessa password non sia utilizzata per accedere a diversi sistemi;
- Non scrivere la password chiaramente su un foglio né condividerla.

Tenuta del registro dei trattamenti (art. 30 GDPR)

Il registro dei trattamenti contiene le informazioni di cui all'art. 30, GDPR (*General Data Protection Regulation*) relative alle operazioni di trattamento svolte nell'ambito delle attività dello studio legale. Attraverso il registro è possibile comprendere come i dati personali dei clienti siano gestiti, al fine di valutare i rischi e permettere al titolare del trattamento (c.d. *accountability*, art. 5, par. 2, GDPR) di adottare le misure di sicurezza tecniche e organizzative adeguate.

In generale sono obbligati alla tenuta del registro tutti i Titolari e i Responsabili che effettuino un trattamento di dati personali non occasionale. Quasi sempre il trattamento degli studi legali ha ad oggetto dati appartenenti a categorie particolari, ossia quelli che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale o quelli che riguardano i dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale (art. 9, par. 1, GDPR) ovvero dati inerenti a condanne penali e reati (art. 10, GDPR). Pertanto, ogni studio legale deve necessariamente dotarsi di un registro dei trattamenti.

Il registro deve contenere tutti gli elementi di cui all'art. 30, par. 1, GDPR e deve essere tenuto costantemente aggiornato, in quanto il suo contenuto deve sempre corrispondere ai trattamenti effettivamente posti in essere.

Definizione di ruoli e responsabilità

- Il personale dipendente e i collaboratori dello Studio legale devono comprendere ruoli e responsabilità per assicurare la gestione della *cybersecurity* e dei rischi associati al trattamento dei dati personali;
- Nei limiti delle risorse disponibili, sarebbe opportuno dotarsi di un responsabile della cybersecurity che faccia rispettare la *policy* dello studio in materia di cyber sicurezza;
- Affidare a un soggetto designato all'interno dello Studio il compito di presidiare la verifica del rispetto delle norme in materia di trattamento dei dati personali, ai sensi dell'art. 2-quaterdecies, c. 1, del D.Lgs. n. 196/2003 (così come modificato dal D.Lgs. n. 101/2018).

Valutazione del rischio e verifiche periodiche

Al fine di compiere una valutazione del rischio, il Titolare del trattamento dovrebbe:

- Identificare le risorse dello Studio connesse alla rete, come, ad esempio, una banca dati contente dati dei clienti o la banca dati delle risorse umane, con i dati personali dei collaboratori/dipendenti e dei fornitori;
- Identificare le minacce, interne ed esterne, accidentali o malevole;
- Identificare le vulnerabilità del sistema;
- Tener conto del rischio che si verifichi una violazione di sicurezza che possa comportare un data breach;
- Tener conto dell'impatto legale, economico e reputazionale che un data breach può avere sullo Studio.

Oltre alle suddette valutazioni, il Titolare dovrebbe prendere in considerazione:

- Lo stato delle misure di sicurezza, tecnologiche e organizzative dello Studio;
- Quali siano le diverse categorie di dati personali gestiti dallo Studio, in modo da definire rispettivamente un adeguato livello di protezione;
- La ripetizione periodica della valutazione dei rischi (almeno una volta/anno).

Infine, il Titolare del trattamento dovrebbe compiere:

- Valutazioni sulle vulnerabilità, al fine di individuare delle criticità nelle difese tecnologiche dello Studio;
- Valutazioni sulla potenziale compromissione di dati, in caso di eventuale *data breach*;
- Svolgimento di *penetration test*, utilizzando un fornitore di servizi di sicurezza che cerchi di *hackerare* la rete dello studio ed indentificare potenziali criticità da correggere.

Valutazione d'impatto sulla protezione dei dati (DPIA)

Nel caso in cui un trattamento possa comportare un rischio elevato per i diritti e le libertà delle persone interessate (qualora vi sia un monitoraggio sistematico dei loro comportamenti o per il gran numero di soggetti interessati, di cui sono trattati, ad esempio, dati appartenenti a categorie particolari o relativi a condanne penali o reati), il GDPR obbliga il Titolare a svolgere una valutazione di impatto prima di darvi inizio.

Qualora residui un rischio elevato per i diritti e le libertà degli interessati, nonostante il Titolare abbia individuato le misure tecniche ed organizzative per attenuarlo, sarà necessario consultare l'autorità di controllo (Garante Privacy).

Quando è obbligatoria una DPIA?

In tutti i casi in cui un trattamento può presentare un rischio elevato per i diritti e le libertà degli interessati. Tra questi:

- Trattamenti valutativi o di scoring, compresa la profilazione;
- Decisioni automatizzate che producono significativi effetti giuridici (es. assunzioni, concessioni prestiti, stipula di assunzioni);
- Monitoraggio sistematico (es. videosorveglianza);
- Trattamento di dati appartenenti a categorie particolari o relativi a condanne penali o reati;
- Dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, anziani, richiedenti asilo, ecc.);
- Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es. riconoscimento facciale, device IoT, ecc.).

In presenza di almeno due dei predetti criteri, la DPIA è obbligatoria.

Quando NON è obbligatoria?

Non è obbligatoria una DPIA per i trattamenti che:

- Non presentano un rischio elevato per i diritti e le libertà degli interessati;
- Hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;
- Sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio del 2018 e le cui condizioni (es. soggetto, finalità, ecc.) non hanno subito modifiche;
- Fanno riferimento a norme e regolamenti, dell'Unione europea o di uno Stato membro, per la cui definizione è stata condotta una DPIA.

La DPIA deve essere condotta prima di procedere al trattamento, prevedendo, comunque, un riesame ad intervalli regolari.

Responsabile della DPIA è sempre il Titolare, anche se la conduzione della stessa può essere affidata ad un soggetto terzo, esterno o interno allo studio. Il Titolare monitora lo

svolgimento della DPIA, consultandosi con il DPO (se presente) e, laddove necessario, richiedendo il parere di esperti del settore.

Sviluppo di piani per la continuità dell'attività

In caso di attacco informatico è indispensabile arrivare preparati. Per questo si consiglia di:

- Segmentare con attenzione i sistemi di backup (per evitare che vengano colpiti tutti simultaneamente). Esercitarsi con il recupero dei file da backup;
- Sviluppare un sistema di rete ausiliario nel caso in cui la rete principale non sia disponibile;
- Identificare mezzi di comunicazione alternativi alla rete.

Sviluppo e test di un piano di risposta agli incidenti (*Incident Response Plan* - IRP)

Gli Studi legali strutturati, con un numero elevato di collaboratori e dipendenti, dovrebbero approntare una lista con i nomi e le informazioni dei contatti di emergenza dei membri del team che sono autorizzati a rispondere a una violazione.

Tali soggetti dovranno essere previamente formati in modo da conoscere ruoli e responsabilità, attuando le misure adeguate alla gravità dell'incidente secondo uno schema che definisce le priorità.

L'IRP dovrà, inoltre, contenere i contatti di eventuali consulenti esterni, di cui lo Studio potrebbe aver bisogno per rispondere all'attacco.

In caso di incidente è importante tracciare le fasi della risposta:

- Il team dovrebbe riunirsi per valutare la risposta data, indentificare e documentare ogni informazione che potrebbe essere utile per i futuri incidenti;
- Documentare la causa dell'incidente, l'impatto sull'attività dello studio e le misure adottate per contenerlo;
- Imparare dall'incidente, in modo da migliorare i controlli tecnici, ridefinire se necessario l'IRP e continuare a monitorare e testare le misure di sicurezza adottate.

Data breach (artt. 33 e 34 GDPR)

In caso di una violazione 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 comunque trattati, il GDPR prescrive al Titolare determinati comportamenti.

Alcuni esempi di *data breach*:

- Furto o perdita di dispositivi informatici contenti dati personali;

- L'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- La divulgazione non autorizzata di dati personali;
- L'impossibilità di ai dati per cause accidentali o per attacchi esterni, virus, ecc.;
- La deliberata alterazione dei dati personali.

Comportamenti da tenere in caso di data breach

1. Notifica al Garante

Soggetto tenuto a effettuarla

Il Titolare del trattamento. L'eventuale Responsabile del trattamento coinvolto è tenuto a informare tempestivamente il Titolare una volta venuto a conoscenza della violazione.

Quando

Senza ingiustificato ritardo e comunque entro 72 ore dal momento in cui il Titolare è venuto a conoscenza della violazione. Trascorso questo intervallo di tempo, il Titolare dovrà giustificare i motivi del ritardo all'atto della notifica all'Autorità Garante per la protezione dei dati personali.

Eccezioni

Non è richiesta la notifica all'Autorità Garante qualora sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche.

Tipi di violazioni di dati personali da notificare

Tutte quelle tipologie che possono avere effetti avversi significativi sugli individui, causando danni fisici, materiali e/o immateriali.

Quali informazioni deve contenere la notifica al Garante e come inviarla

La notifica deve contenere le informazioni previste all'art. 33, par. 3 del GDPR. Qualora si utilizzi per la notifica il modello predisposto dal Garante, è necessario scaricarlo sul proprio dispositivo e successivamente procedere alla sua compilazione.

La notifica deve essere inviata al Garante tramite posta elettronica all'indirizzo **protocollo@pec.gpdp.it** e deve essere sottoscritta digitalmente (con firma elettronica qualificata/firma digitale) ovvero con firma autografa. In quest'ultimo caso la notifica deve essere presentata unitamente alla copia del documento d'identità del firmatario.

2. Comunicazione agli interessati.

Se la violazione comporta un rischio elevato per i diritti delle persone, il Titolare deve comunicarla a tutti gli interessati, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurne l'impatto.

3. Registro delle violazioni.

Tutte le volte in cui si verifica una violazione, a prescindere dalla notifica all'Autorità Garante, il Titolare del trattamento deve documentarla predisponendo un apposito registro, al fine di consentire all'Autorità di effettuare eventuali controlli sul rispetto della normativa.

Formazione e test

- Organizzare corsi di formazione periodici per tutti i dipendenti/collaboratori, avvalendosi di enti di formazione accreditati;
- Effettuare stress test e altre valutazioni di impatto delle minacce per testare la sicurezza e i tempi di risposta, almeno una volta l'anno.

Assicurazione per la responsabilità da attacchi informatici

Anche se uno Studio legale implementa i migliori processi e tecnologie di sicurezza informatica, resterà comunque esposto ad un certo livello di rischio.

Pertanto, dopo aver valutato l'esposizione al rischio, uno studio legale dovrebbe prendere in considerazione una polizza assicurativa che copra il rischio residuo di attacchi informatici, in modo da sostenere i costi di un eventuale *data breach*.

Formazione del personale

Le persone sono spesso l'anello debole nella sicurezza informatica. La mancanza di conoscenze o la semplice disattenzione sono elementi che i cybercriminali sfruttano a loro vantaggio. La maggior parte degli attacchi sono studiati in modo da apparire assolutamente legali, ma contengono link attraverso cui possono essere ottenute informazioni riservate, quali username, password, dettagli sulle carte di credito. Gli hacker preferiscono questo tipo di attacchi perché sono molto più efficienti rispetto alla violazione dei sistemi di sicurezza di un computer.

Per questa ragione è fondamentale che tutti i membri di uno Studio legale conoscano le forme più comuni di un attacco informatico e siano formati per rispondere adeguatamente a tali attacchi. Se possibile, sarebbe utile testare il personale con simulazioni di phishing e verificare quale sia il livello di consapevolezza rispetto alla sicurezza informatica.

Inoltre, occorre considerare che i dipendenti e i collaboratori dello studio legale, in qualità di autorizzati al trattamento ai sensi dell'art. 29 del GDPR, devono obbligatoriamente ricevere le adeguate istruzioni e la formazione necessaria al corretto trattamento di dati personali, nell'esecuzione delle prestazioni lavorative.

In effetti, l'obbligo di fornire le adeguate istruzioni agli autorizzati al trattamento e la necessaria formazione in materia di protezione di dati personali ricade espressamente in capo al Titolare del trattamento, ai sensi del citato art. 29 GDPR.

La formazione del personale dello studio legale, dunque, oltre alle norme del GDPR e alle necessarie istruzioni per procedere al corretto trattamento dei dati personali, dovrebbe avere ad oggetto anche le regole della sicurezza informatica.

Cos'è la sicurezza informatica

La sicurezza informatica è quell'insieme di procedure che permettono di difendersi dall'uso illegale, non autorizzato o negligente dei dati informatici.

Il personale dipendente e i collaboratori devono essere consapevoli che un attacco può essere esplicito o utilizzando artifizi e raggiri (es. il phishing).

Perché la sicurezza informatica è importante

Il personale deve essere consapevole che:

- I dati memorizzati nelle banche dati, comprese quelle degli studi legali, acquisiscono sempre maggior valore e gli attacchi informatici si fanno più sofisticati e frequenti;

- Gli attacchi informatici potrebbero avere delle implicazioni legali, a causa del fatto che gli avvocati sono tenuti a rispettare la riservatezza dei dati relativi ai loro clienti o di cui sono venuti in possesso nello svolgimento dell'attività professionale;
- Sussistono dei rischi di natura economica e reputazionale associati a una violazione della sicurezza informatica;
- Occorre essere formati per rispondere ad un attacco informatico ed evitare perdite future;
- È necessario acquisire familiarità con l'IRP dello studio (laddove disponibile), in particolare sulle procedure da attuare.

Alcuni esempi di minacce comuni

Il personale deve conoscere i differenti tipi di attacco informatico che potrebbero trovarsi ad affrontare con maggiore frequenza in uno studio legale. Fra questi si ricordano:

- Malware: software malevoli come virus, worms, trojan horses, spyware e adware;
- Ransomware: questi software sono in grado di criptare o bloccare i dati e successivamente viene chiesto un pagamento (in genere in bitcoin) per ottenere la chiave di cifrature e accedere nuovamente ai dati;
- Phishing/spear phishing/whaling emails: si tratta di attacchi realizzati attraverso mail apparentemente legittime, contenenti link infettati con un malware o che cercano di carpire informazioni personali o finanziarie dal destinatario;
- Attacchi denial-of-service (DoS): attacchi informatici in cui si sovraccarica un dispositivo con un numero elevato di richieste fino a renderlo inutilizzabile;
- Furto di identità digitale: l'identità digitale è l'insieme dei dati informatici che identificano in maniera univoca una persona fisica, giuridica o un dispositivo online. Sfruttando la tecnica del phishing, un hacker potrebbe utilizzare l'account di un avvocato e indurre un altro soggetto ad effettuare un pagamento.
- Vulnerabilità cc.dd. zero-day: si tratta di vulnerabilità del codice di un software non ancora conosciute e che possono essere sfruttate dagli hacker che per primi le scoprono.

INFOGRAFICA: Consigli e Suggerimenti