

Attacchi hacker verso gli Studi Legali in forte aumento: perchè?

**Piccola guida sull'importanza
di proteggere i dati dei tuoi clienti**



Sempre di più spesso gli **hacker** prendono di mira gli **Studi Legali** perché sono una fonte importante di dati sensibili e preziosi (*finanziari* - come nel caso di fusioni e acquisizioni, *personali* e *strategici*), rendendoli obiettivi di ricatti (ransomware), furto di identità, frodi, insider trading, e per ottenere vantaggi nelle controversie legali.

La **reputazione** di uno Studio Legale è molto sensibile ai **disastri IT** che causano esfiltrazioni di dati sensibili. E, oltre alla fiducia dei clienti, le violazioni portano a **perdite** economiche e finanziarie causate dalle **sanzioni** legali (GDPR).

In caso di incidente IT, il tuo Studio Legale sarebbe in grado di dimostrare di aver applicato ogni possibile protezione in modo costante e sicuro?

I tuoi avvocati sarebbero nelle condizioni di riprendere il lavoro senza interruzioni (Disaster Recovery Plan e Business Continuity)?



Le minacce informatiche ad Avvocati e Studi Legali:

La violazione dell'integrità dei dati sensibili e strategici custoditi da uno Studio Legale ha gravi ripercussioni sul successo di un caso e sulla vita dei clienti, delle aziende e delle persone coinvolte nelle controversie legali. Inoltre, un incidente IT può causare il rallentamento o il blocco delle prestazioni: pensiamo a uno Studio Legale sotto attacco hacker che deve mettere in discussione scadenze e documenti strategici da cui dipende il successo di un caso in tribunale.

I rischi più ricorrenti nel settore legale sono:

1. **Furto di dati sensibili e riservati** per rivenderli sul dark web, per manometterli e/o per furti di identità e frodi.
2. **Diffusione di informazioni critiche riservate** con conseguente danno di immagine per lo Studio, sanzioni dal Garante della Privacy e pesanti implicazioni legali.
3. **Rischio Ransomware** quando i cybercriminali criptano i dati dei clienti e chiedono un riscatto per sbloccarli.

Questione di sicurezza (ma anche di reputazione)



Una riflessione: quando si parla di **giustizia** entrano in gioco anche le emozioni e quel bisogno di protezione eassicurazione che ci aspettiamo da uno Studio Legale e dai suoi Avvocati e Consulenti. Uno Studio sotto **attacco hacker** dovrà gestire quindi, sia il grande problema del furto di dati sensibili e della loro manomissione, sia la questione reputazionale legata alla **fiducia** dei clienti: se uno Studio Legale viene percepito come “non sicuro” i clienti saranno preoccupati, amareggiati e insoddisfatti, e potranno rivolgersi ad un altro Studio che riserva maggiore attenzione alla **protezione dei dati confidenziali** oltre che strategici.

Far sapere che proteggi i dati sensibili con sistemi sempre aggiornati ed efficienti ti aiuterà a instaurare un rapporto di fiducia a 360 gradi con i tuoi clienti.

*CONSIGLIO: Investi in **cybersecurity** e rendi partecipe i tuoi clienti di questa **attenzione** alla loro **privacy**, che sarà molto apprezzata.*

Cybersecurity per Studi Legali e Avvocati: come proteggersi

A. Praticare l'igiene informatica

Si tratta di un insieme di buone pratiche interne che riducono il rischio legato a virus e attacchi hacker. Molto spesso la fonte di un virus è proprio la chiavetta usb di un collaboratore, lo sapevi? Anche le e-mail di phishing vengono inconsapevolmente attivate dal personale interno. Ecco perché occuparsi della formazione interna (cyber awareness) sui rischi e sulle norme di igiene informatica è il primo passo da compiere (Core Up propone corsi personalizzati).

Core Up Srl suggerisce agli Avvocati e ai loro Studi di compiere le seguenti azioni strategiche:



B. Scegliere un MSP

Per la **gestione**, il **monitoraggio** e la **salute** dell'ambiente IT dello Studio Legale si può incaricare un MSP Managed Service Provider (Provider di servizi gestiti) che **da remoto e 24/7 controlla** lo stato delle reti e dei sistemi. Un MSP compie tutte quelle azioni necessarie a tenere il più possibile in sicurezza l'infrastruttura IT (rinnovo dell'antivirus, installazione di firewall, manutenzione hardware...) e, in caso di attacco o problemi, interviene tempestivamente per riportare la situazione alla normalità.

C. Verificare la sicurezza dell'infrastruttura IT

Per identificare le minacce IT e mitigarne i rischi, è fondamentale partire da una **valutazione della sicurezza** dell'infrastruttura attraverso due tipologie di verifica: il Vulnerability Assessment e il Penetration Test sono metodologie (complementari e consequenziali) che permettono di realizzare un **Security Program** su misura, efficace ed efficiente. (Un MSP si occupa anche di questo!)

D. Studiare una strategia di gestione in caso di incidenti IT

Pensare a un piano di azione concreto ed efficiente aiuta a **mitigare i problemi** in caso di incidenti informatici che mandino in tilt i sistemi IT con conseguente perdita dei dati o furto di informazioni sensibili. (Anche in questo caso scegliere un MSP si rivela una scelta vincente!).

E se capitasse al tuo Studio Legale?



2026, Gian Gaetano Bellavia, Italia

Bellavia, consulente in indagini di criminalità economica e noto anche per le sue partecipazioni televisive come esperto, ha subito il furto di 910 gigabyte di file “ad alta sensibilità” con implicazioni a cascata per tutti i nomi coinvolti (studi legali, giornalisti, consulenti, collaboratori).

2021, Studio Legale Allens, Australia

Una sofisticata violazione della sicurezza informatica ha permesso agli hacker di attaccare lo Studio attraverso un sistema di archiviazione e trasferimento dei file, ormai vecchio di 20 anni, non aggiornato e, quindi, non sicuro.

2019, Avvocato di Milano (nome non specificato)

Caso di *Sim Swapping* (clonazione di una SIM) che è costato oltre € 200.000 all'Avvocato vittima e, dopo condanna del Tribunale di Milano, un ingente risarcimento all'istituto bancario e all'operatore di telefonia per la carenza di misure di autenticazione.

2017, DLA Piper, a livello globale

Attaccata da un ransomware che ha debilitato migliaia di suoi computer, DLA Piper si è trovata costretta a chiudere le sue operazioni digitali a livello globale. I sistemi di posta elettronica e telefono sono stati disabilitati, costringendo avvocati e altri dipendenti a lavorare utilizzando i propri telefoni cellulari, esponendo così potenzialmente la società ad altri rischi.

Core Up: il tuo MSP, e non solo...

Scegliere un **partner tecnologico MSP** come Core Up, che propone il noleggio e la vendita di hardware e software per l'ufficio e servizi di monitoraggio, assistenza e gestione proattiva dell'infrastruttura IT, **aumenta i livelli di sicurezza** del tuo Studio Legale, riducendo al minimo i tempi di down-time e i disservizi.

Così potrai ottimizzare tempi e costi, il tutto gestito con comodi canoni periodici personalizzabili.

Cosa possiamo fare per te:

- **SERVIZIO DI MSP (MANAGED SERVICE PROVIDER)**
- **NOLEGGIO DI PC, SERVER, STORAGE, STAMPANTI E MULTIFUNZIONI**
(approfondimento nella pagina successiva: [Accordo Utax/Cassa Forense](#))
- **TELEFONIA E CONNETTIVITÀ**

Contattaci per maggiori informazioni: sarà un piacere conoscere la tua realtà e consigliarti i migliori strumenti per far crescere il tuo Studio:

T. 030.4194040

M. info@coreup.it / segreteria@coreup.it

W. www.coreup.it

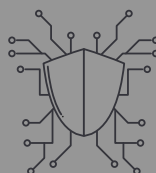


Accordo Utax / Cassa Forense

Cassa Forense ha sottoscritto con **Utax**, brand leader nel settore dell'Office Automation, una convenzione relativa ai sistemi di stampa e alla tecnologia Blockchain/Rfid.

Core Up è rivenditrice delle stampanti e delle multifunzioni Utax. Possiamo, quindi, garantire agli Studi Legali l'applicazione della convenzione che prevede prezzi speciali per i sistemi di stampa.

Con i sistemi Utax è possibile Certificare e Notarizzare documenti importanti tramite Blockchain con un semplice processo di stampa. Questa nuova tecnologia garantisce l'unicità, l'inalterabilità, la tracciabilità (fisica e digitale) e la data certa della generazione di un documento.



I vantaggi del nostro noleggio operativo di stampanti e multifunzioni:



- Costi certi con comodi **canoni** periodici e personalizzabili
- **Rifornimento automatico** dei toner
- **Assistenza** da remoto e on-site compresa
- **Monitoraggio** da remoto della salute della macchina
- **Referente unico** per tutto il parco macchine stampa (risparmi tempo/denaro)
- Nessuna gestione dei **cespiti**
- Possibilità di attivare il servizio di **smaltimento** dei toner esausti



Contattaci per un sopralluogo gratuito, un preventivo e uno studio del Vostro fabbisogno di stampa:

T. 030.4194040

M. segreteria@coreup.it



Contattaci per maggiori informazioni: sarà un piacere conoscere la tua realtà e consigliarti i migliori strumenti per far crescere il tuo Studio.

T. 030.4194040

M. info@coreup.it / segreteria@coreup.it

W. www.coreup.it

seguici su LinkedIn:

