

Aumentano gli attacchi hacker verso gli Studi di Commercialisti: perché?



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

Sempre più spesso gli **hacker** prendono di mira gli **Studi di Consulenza e i Commercialisti** perché sono una fonte importante di dati sensibili e preziosi (*fiscali, patrimoniali, finanziari*) che li rendono obiettivi di ricatti (ransomware), furti di identità e frodi a danno dei propri clienti, del loro patrimonio e della privacy.

La **reputazione** di uno Studio di Commercialisti 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 sarebbe in grado di dimostrare di aver applicato ogni possibile protezione in modo costante?

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



Le minacce informatiche a Commercialisti e Studi Professionali:

La violazione dell'integrità dei dati sensibili e strategici custoditi da un **Commercialista** ha gravi ripercussioni sulla **sicurezza**, sul patrimonio e sulla vita dei clienti, privati o aziende che siano. Immaginate se i dati sensibili di un cliente venissero usati per un furto d'identità o per accedere ai suoi conti correnti bancari! Inoltre, un incidente IT può causare il rallentamento o il blocco delle prestazioni: pensiamo a uno Studio di Commercialisti sotto attacco hacker che deve mettere in discussione le **scadenze fiscali** dei suoi clienti, andando incontro a perdita della fiducia e a possibili sanzioni.

I rischi IT più ricorrenti per un Commercialista 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 fiscali e 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)

Perché i Commercialisti sono un bersaglio:

- **Miniere di dati sensibili:** I Commercialisti gestiscono informazioni cruciali di aziende e privati (fiscali, patrimoniali, finanziari), custodendo codici fiscali, partite IVA, dettagli bancari, bilanci e informazioni societarie riservate (rivendibili sul dark web con alti profitti per gli hacker).
- **Vulnerabilità delle infrastrutture:** Molti Studi Professionali, soprattutto i più piccoli, hanno risorse limitate per la cybersecurity, diventando quindi obiettivi "facili" da attaccare.
- **Accesso a fondi finanziari:** Capita molto spesso che gli hacker usino i dati rubati ai Commercialisti per sostituirsi al professionista e indurre i clienti a trasferire denaro o per effettuare truffe fiscali.
- **Social Engineering:** Il rapporto di fiducia che si instaura tra cliente e Commercialista viene sfruttato dagli hacker per carpire informazioni o per rubare denaro, ad esempio attraverso false e-mail (phishing) in cui l'hacker si finge il Commercialista e chiede urgentemente di effettuare un bonifico.
- **Ransomware ad alto impatto:** Criptare i dati di uno Studio Commercialista blocca l'operatività, spingendo i professionisti a pagare il riscatto per evitare interruzioni dell'attività, danni alla reputazione e sanzioni per violazione del GDPR.

Una riflessione: quando si parla di **bilanci, tasse, gestione economica e fisco** non si sta parlando solo di numeri e importi, bensì anche della vita, dell'impegno e dei sacrifici delle persone. Diventa comprensibile, quindi, che un Commercialista risponda anche a quel bisogno di tutela e assicurazione che porta inevitabilmente alla costruzione di un legame di fiducia. Uno Studio di Commercialisti sotto **attacco hacker** dovrà gestire 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 di Professionisti e Consulenti 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 Professionali e Commercialisti: come proteggersi

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



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).

B. Scegliere un MSP

Per la **gestione**, il **monitoraggio** e la **salute** dell'ambiente IT del tuo Studio 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!).

Managed Service Provider (MSP): chi è?

Un MSP aiuta a **proteggere i dati sensibili** e il know-how aziendale con il monitoraggio costante dell'ambiente IT, la manutenzione e la gestione proattiva.

In caso di attacchi o disastri IT l'azienda riparte nel minor tempo possibile, riducendo quindi i **tempi di fermo** e le perdite economico-finanziarie.

Offre servizi altamente specializzati su base contrattuale, spesso con un **canone** mensile/annuale, permettendo al cliente di esternalizzare le complessità tecnologiche e concentrarsi sul proprio core business.

Dati sensibili al sicuro: Imprenditori liberi di concentrarsi sul fatturato

Quando hai un partner IT con funzione di MSP puoi contare su un'infrastruttura IT **efficiente e sicura** mentre ti dedichi al tuo lavoro.

In caso di incidente IT dovuto a un attacco hacker, a un errore umano o a un disastro naturale, un MSP ti aiuta a contenere i danni e le perdite perché ti permette di ripartire nel minor tempo possibile, scongiurando i tanto temuti down-time.

Inoltre, se scegli un MSP che fornisce anche hardware e software, avrai un parco macchine IT sempre aggiornato e performante.

I vantaggi per le aziende che scelgono un MSP:

- Continuità operativa e riduzione dei tempi di fermo
- Assistenza telefonica e da remoto illimitata
- Rete IT più sicura e sempre aggiornata
- Unico referente IT: risparmio di tempo/denaro
- Consulenza IT altamente qualificata
- Zero sorprese di spesa: comodo contratto con canoni periodici fissi
- Rinnovo parco macchine con comoda formula noleggio

E se capitasse al tuo Studio di Commercialisti e Consulenti?



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, **studi commercialisti**, consulenti, collaboratori).

2024, Deloitte UK, Gran Bretagna

Azienda multinazionale di consulenza fiscale e revisione contabile è stata vittima di un attacco ransomware che ha compromesso 1 terabyte (TB) di dati sensibili.

2022, Studio Teruzzi Gesis Srl, Italia

Vittima di un tentativo di attacco ransomware, gli hacker hanno cercato di criptare file e sottrarre dati per poi chiedere un **riscatto**. Fortunatamente, grazie alla presenza di sistemi di backup e protezioni perimetrali, i danni furono contenuti: fu esfiltrato solo il 7% dei dati.

“Noi siamo piccoli, a noi non capita.”

“Abbiamo l'antivirus, siamo tranquilli.”

“Tanto facciamo il backup su hard disk.”

Queste frasi rappresentano un rischio per molti Studi.

**Nessuno è troppo piccolo per essere attaccato:
le minacce informatiche ormai si muovono in modo
automatizzato, colpendo chiunque abbia una
vulnerabilità aperta, indipendentemente
da dimensione o fatturato.**

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, 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)** per il monitoraggio e la gestione proattiva della tua infrastruttura IT
- **NOLEGGIO DI PC, SERVER, STORAGE, STAMPANTI E MULTIFUNZIONI** con comodi canoni periodici personalizzabili per un ambiente IT sempre aggiornato e performante
- **TELEFONIA E CONNETTIVITÀ**
- **TECNOLOGIE PER MEETING ROOM**



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 di LinkedIn:

