Image

CAMMINO DIRITTO
Rivista di informazione giuridica
https://rivista.camminodiritto.it

IL FINTECH: LA GALLINA DALLE UOVA D'ORO PER GLI HACKER

Il settore bancario è sempre stato un obiettivo redditizio per i criminali. Questo avviene truffando i clienti o attaccando direttamente gli istituti finanziari. Il FinTech ha reso l'attività bancaria più semplice per i clienti, ma i criminali informatici hanno questo settore nei loro radar. Nel corso degli anni, le tattiche sono leggermente cambiate, dalle tecniche smash-and-grab ai sofisticati trojan bancari di oggi. La criminalità organizzata continua ad evolversi e i gruppi criminali sono ora più che mai in grado di utilizzare gli strumenti di hacking più aggiornati. Le banche tradizionali e le società FinTech devono camminare insieme per garantire che l'open banking rimanga sicuro. Il riciclaggio di denaro si evolve e assume nuove forme più insidiose.

di **Loris Taffi**
IUS/05 - DIRITTO DELL'ECONOMIA
Articolo divulgativo - ISSN 2421-7123

Direttore responsabile
Alessio Giaquinto

Pubblicato, Lunedì 2 Dicembre 2024

CamminoDiritto.it
ISSN 2421-7123

Abstract ENG

Banking has always been a lucrative target for criminals. It be through scamming customers out of their money, or directly attacking the financial institutions. FinTech has made banking easier for customers, but cyber criminals have this industry in their radars. Over the years, tactics have changed somewhat, from the smash-and-grab techniques to the sophisticated banking trojans of today. Organised crime continues to evolve and criminal groups are capable now more than ever to use the latest hacking tools. Traditional banks and FinTech companies need to walk together to ensure that open banking remains safe. The money laundering changes his face and becomes more hidden.

Sommario: 1. Una sicurezza “by-design”; 2. Il rischio della stabilità finanziaria; 3. Il settore finanziario è bersagliato; 4. Il profilo del cybercriminale; 5. Il ruolo della Blockchain; 6. La trasformazione del riciclaggio di denaro nell’era digitale; 7. Il Digital Market Act e il Digital Service Act a confronto; 8. Conclusioni

1-Una sicurezza “by-design”

La Direttiva dei Sistemi di Pagamento (c.d. PSD2 Direttiva EU 2015/2366) ha trasformato il settore finanziario e ha spinto il potenziale di innovazione tecnologica che ha raggiunto vette enormi quanto entusiasmanti in questo ambito (2). Il settore fintech era già un settore consolidato e, secondo uno studio del 2023 condotto dal Boston Consulting Group, si stima che il volume di affari raggiungerà il valore dei 22mila miliardi di dollari entro il 2030, impiegando oltre 400 milioni di posti di lavoro nel mondo (3). Ma con maggiori accessi, sia ai dati finanziari, sia alla gestione del patrimonio digitale, il settore è probabilmente il più importante a livello tecnologico in questo momento. Tuttavia, allo sviluppo del settore e al progresso tecnologico si aggiungono complessità, rischi e, naturalmente, maggiori possibilità di attacchi informatici. Per sferrare un attacco gli hacker scelgono sempre la strada più semplice e con risorse di sicurezza nettamente inferiori rispetto alle banche tradizionali. Le moderne bande criminali sono le stesse che in passato hanno preso di mira le grandi banche, disponendo già di numerose risorse, dai malware sofisticati alle complesse kill chain. Le preoccupazioni relative alla sicurezza non possono più essere un ripensamento e i dispositivi IoT (Internet of Things) connessi sono l’esempio perfetto di come la sicurezza non possa permettersi di passare in secondo piano nel processo di innovazione. Ma come affrontare il problema della sicurezza dall’interno? Il modo più efficace è adottare una mentalità basata sulla sicurezza fin dalla progettazione dei sistemi informatici. Ciò significa che i problemi di sicurezza vengono sollevati in ogni fase del processo, dalla pianificazione iniziale fino alla messa in funzione. Il software ne è un ottimo esempio e incorporando la sicurezza in tutte le fasi

CamminoDiritto.it
ISSN 2421-7123

non solo si sviluppa un prodotto finale più sicuro, ma i bug (di sicurezza e funzionali) possono essere risolti più velocemente e a un costo inferiore se vengono rilevati nelle prime fasi del ciclo di vita dello sviluppo del software. Assistiamo continuamente ad esempi di sicurezza che arrivano troppo (a volte appena prima del rilascio del prodotto). Il risultato è, purtroppo, l'identificazione di un gran numero di vulnerabilità. Ciò a sua volta comporta costosi lavori di riparazione e ulteriori test. Questi cicli continui di pen-testing, correzione e ripetizione del test non solo possono essere costosi, ma spesso possono avere un impatto sulle scadenze di rilascio, con conseguenti disagi per l'utente finale.

2. Il rischio della stabilità finanziaria internazionale

Stando ad un recente rapporto del Fondo monetario internazionale (FMI), la stabilità finanziaria globale è minacciata dalla crescente frequenza e sofisticatezza degli attacchi informatici (4). Anche il rischio di perdite estreme derivanti da attacchi informatici è in aumento, osserva il rapporto, lasciando il settore finanziario esposto in modo unico alle minacce informatiche, poiché le operazioni coinvolgono grandi quantità di dati e transazioni sensibili. Per gli istituti finanziari, il risultato di un attacco informatico potrebbe assumere i connotati che vanno dai danni alla reputazione sino al default. Inoltre, gli esperti avvertono che per il settore finanziario nel suo complesso, grandi attacchi potrebbero minare la fiducia nel sistema, interrompere servizi critici e estendersi ad altri settori. Negli ultimi due decenni quasi un quinto degli incidenti informatici segnalati ha colpito il settore finanziario globale, causando perdite dirette per 12 miliardi di dollari alle società finanziarie. Dal 2020, le perdite dirette ammontano a circa 2,5 miliardi di dollari. Il rapporto del FMI aggiunge che le banche sono particolarmente prese di mira e che le cifre sulle perdite sono probabilmente molto più elevate se si considerano le perdite indirette e i danni alla reputazione. Gli incidenti informatici rappresentano un rischio operativo chiave che potrebbe minacciare l'area macrofinanziaria complessiva. Inoltre nel report, si legge che sebbene finora gli incidenti informatici non siano stati sistemici, la combinazione tra una rapida trasformazione digitale, l'innovazione tecnologica (come intelligenza artificiale) e l'acuirsi delle tensioni geopolitiche globali, aggraverebbero il rischio. Il rapporto del FMI esorta le società finanziarie a rafforzare la propria capacità di sicurezza informatica attraverso stress test e accordi di condivisione delle informazioni. Inoltre, il Fondo monetario internazionale invita le autorità a sviluppare strategie nazionali di sicurezza informatica adeguate e adeguate, accompagnate da quadri normativi.

3. Il settore finanziario è bersagliato

Il guadagno facile è uno dei motivi principali per cui il settore finanziario viene spesso preso di mira, così come la maggior parte degli attacchi informatici in tutti i settori. Poiché i dati finanziari sono il fulcro del settore finanziario, qualsiasi attacco al sistema

CamminoDiritto.it
ISSN 2421-7123

può paralizzare qualsiasi azienda. Gli hacker cercano anche aziende che hanno maggiori probabilità di pagare un riscatto per riavere i propri dati e cercano aziende che dispongono dei dati più preziosi da vendere sul dark web. Quali sono i motivi?

3.1 Il denaro

Il denaro è la motivazione numero uno per la maggior parte degli hacker. Il settore finanziario, che comprende assicuratori, banche e consulenti finanziari, è un obiettivo enorme per coloro che sono motivati principalmente dal fare soldi. L'hacking di organizzazioni finanziarie può potenzialmente consentire ad autori di minacce malintenzionate di accedere ad account o informazioni personali che possono aiutare un criminale a ottenere accessi non autorizzati ed effettuare transazioni finanziarie o indurre altri a rivelare ulteriori informazioni e inviare loro denaro.

3.2 Dati personali e dati sensibili

Le istituzioni finanziarie utilizzano i dati per fornire prodotti e servizi migliori ai clienti. Questi dati, tuttavia, sono spesso dati sensibili o personali, come le informazioni di identificazione personale, che attirano l'attenzione dei criminali informatici. Le compagnie assicurative, ad esempio, in genere raccolgono ed elaborano grandi quantità di dati personali per comprendere le esigenze dei propri clienti e fornire prodotti personalizzati in base al loro stile di vita, dati demografici, rischi e altri fattori. Questo tipo di dati può essere prezioso per i criminali informatici, che possono utilizzarli per creare tentativi di phishing più accurati, minacciare di distruggere o condividere i dati come parte di un attacco ransomware.

3.3 Evoluzione digitale

La pandemia di COVID-19 ha accelerato significativamente la trasformazione digitale. Durante questo periodo di confinamento sociale volontario e obbligatorio, la domanda di servizi finanziari online è aumentata in modo massiccio. Questa esigenza è stata soddisfatta dalle organizzazioni che hanno adottato nuovi processi, flussi di lavoro e tecnologie. Le nuove tecnologie, come la blockchain e i rivoluzionari che hanno modernizzato i sistemi di pagamento, hanno portato a rapidi cambiamenti nel settore. I rapidi cambiamenti spesso coincidono con l'aumento dei problemi di sicurezza informatica poiché le aziende avanzano con soluzioni tecnologiche e non considerano le implicazioni sulla sicurezza IT se non molto tempo dopo. Con un numero sempre maggiore di persone che accedono alle proprie informazioni finanziarie online, gli hacker e altri criminali informatici hanno avuto più persone e aziende da prendere di mira.

CamminoDiritto.it
ISSN 2421-7123

3.4 Ransomware e criptovalute

Secondo l'internet Crime Report dell'FBI (5), le bande di ransomware potrebbero aver violato più di 870 organizzazioni di infrastrutture critiche nel 2022. Organizzazioni di tutti i settori hanno presentato oltre 2300 reclami, per un totale di circa 35 milioni di dollari di perdite. Inoltre, le aziende di servizi finanziari sono tra i settori infrastrutturali più colpiti dal ransomware, dietro solo a pochi leader di questo gruppo: aziende tecnologiche, governo, produzione critica e sanità. L'FBI incoraggia le vittime del ransomware a non pagare il riscatto adoperando criptovalute, perché ciò motiva i malintenzionati a continuare le loro attività e attira nuovi criminali informatici. Inoltre, non vi è alcuna garanzia che le vittime recuperino i propri dati. Ad esempio, negli ultimi anni, la Corea del Nord è stata collegata al furto di miliardi di dollari, in gran parte in asset virtuali e criptovalute.

4. Il profilo del cybercriminale

I criminali informatici sono generalmente motivati dal profitto finanziario e vedono il settore finanziario come un'opportunità per separare i clienti e i proprietari di un'azienda finanziaria dai loro soldi. Possono concentrarsi su attacchi, come phishing o ransomware, per ottenere credenziali di accesso e utilizzarle per effettuare transazioni non autorizzate.

4.1 Hacktivisti

Gli hacktivisti sono hacker politicamente motivati. Possono prendere di mira il settore finanziario per ragioni ideologiche e mirare a provocare disagi. Le loro attività possono comportare furti, ma è più probabile che l'obiettivo sottostante sia il disagio causato dal furto. Gli attacchi DDoS, ad esempio, sono efficaci nel causare interruzioni dell'attività, soprattutto quando coincidono con un periodo particolarmente intenso (come ad esempio il Black Friday). Se i clienti bancari non possono accedere ai propri soldi su richiesta, ciò può portare a una significativa perdita di fiducia nell'organizzazione finanziaria, segnando una vittoria per gli hacktivisti che desiderano indebolire determinate istituzioni o ideologie. Un hacktivista può anche utilizzare attacchi informatici per effettuare violazioni dei dati per far trapelare informazioni sensibili, danneggiare la reputazione di un'organizzazione e potenzialmente rivelare informazioni che la screditano agli occhi del pubblico e dei suoi colleghi.

4.2 Minacce interne

Nel caso di una minaccia interna, l'autore della minaccia ha una conoscenza privilegiata

CamminoDiritto.it
ISSN 2421-7123

di come opera l'azienda e potrebbe già avere le credenziali necessarie per accedere ai dati sensibili. Ciò rende più semplice per loro rubare, divulgare e modificare dati riservati o cruciali. La minaccia interna è particolarmente significativa nel settore finanziario. Tutto il personale deve lavorare eticamente per garantire la sicurezza dei dati quando lavora con ingenti somme di denaro e informazioni personali. Inoltre, devono essere predisposti controlli di sicurezza per monitorare e limitare l'accesso ai dati più preziosi.

4.3 Terrorismo

Gli attacchi da parte dei gruppi terroristici sono tipicamente geopolitici e ideologici. A causa delle motivazioni e delle risorse disponibili, tali attacchi possono essere sofisticati, persistenti e gravemente dannosi, non solo per le singole imprese interessate, ma per l'intero settore o per l'economia. I gruppi di hacker sponsorizzati dai terroristi e dai fondamentalisti possono mirare ad accedere alle reti finanziarie e a rubare o corrompere dati a scopo di lucro, ma anche a causare interruzioni, danneggiare irrevocabilmente gli archivi a scopo di spionaggio. Il cyberterrorismo potrebbe implicare il prendere di mira i sistemi di pagamento per causare diffusi disagi economici.

5. Il ruolo della Blockchain

La Blockchain è una tecnologia decentralizzata e distribuita che facilita la tenuta dei registri delle transazioni. La letteratura la definisce come sicura, trasparente e a prova di manomissione (6). È costituito da una catena di blocchi, in cui ciascun blocco contiene un elenco di transazioni ed è posizionato in ordine cronologico. Questi blocchi sono collegati tramite hash crittografici, formando una catena continua e immutabile. Poiché questi blocchi sono immutabili, la fiducia è richiesta principalmente quando un utente o un programma immette dati. I principali aspetti favorevoli della Blockchain sono: decentralità rispetto ad una autorità statale, trasparenza, immutabilità, velocità di fruizione, integrità costante dei dati e innovazione. Al contrario, ad oggi possiamo notare questi aspetti negativi: consumo di energia, forte anonimato e quasi assenza di regolamenti che ne disciplinano l'utilizzo. Le blockchain hanno un'architettura su larga scala con molti livelli, come consenso, contratti intelligenti, reti e client endpoint. Questi livelli sono spesso presi di mira dagli attacchi informatici, esponendola ad un'ampia varietà di vulnerabilità. Due macro minacce informatiche che devono essere considerate per quanto riguarda la blockchain (nelle transazioni finanziarie) possono essere:

minaccia al protocollo di consenso: i protocolli di consenso sono adoperati per raggiungere un accordo tra i partecipanti quando si aggiunge un nuovo blocco. Poiché non esiste un'autorità centrale, le vulnerabilità del protocollo di consenso minacciano di controllare una rete blockchain e dettare le sue decisioni consensuali da vari vettori di

CamminoDiritto.it
ISSN 2421-7123

attacco. Il protocollo di consenso deve essere valutato e testato adeguatamente per garantire che raggiunga sempre la risoluzione prevista; violazione della privacy: le blockchain sono trasparenti per natura e i partecipanti possono condividere dati che i malintenzionati possono utilizzare per dedurre informazioni riservate o sensibili. Le organizzazioni devono valutare attentamente il proprio utilizzo della blockchain per garantire che vengano condivisi solo i dati consentiti senza esporre informazioni private o sensibili.

6. La trasformazione del riciclaggio di denaro nell'era digitale

Lo sviluppo della tecnologia consente alle persone di raggiungere quasi tutte le opportunità attraverso Internet. I sistemi bancari aperti offrono ai consumatori l'opportunità di interagire con le istituzioni finanziarie, insieme a portafogli mobili 24 ore su 24, 7 giorni su 7. Questo sviluppo del settore finanziario ha portato con sé nuove minacce di riciclaggio di denaro, soprattutto per quanto riguarda l'uso diffuso di dispositivi mobili, e aumenta il tasso e l'effetto dei reati di riciclaggio di denaro. Inoltre, è un dato di fatto che con l'aumento dei crimini finanziari come il riciclaggio di denaro e il finanziamento del terrorismo, le normative globali o locali cambiano (7). Il riciclaggio di denaro esiste da secoli e i criminali hanno sviluppato numerosi metodi per mascherare i loro profitti illeciti: contrabbando di denaro contante, prestanome, compagnie di comodo e attività immobiliari sono soltanto alcuni esempi. I metodi spesso implicano lo spostamento di denaro attraverso più conti e giurisdizioni, rendendo difficile per le forze dell'ordine tenere traccia dei fondi. Tali tecniche illegali e tradizionali di riciclaggio di denaro sono ancora in uso oggi, ma l'ascesa delle valute digitali e della tecnologia blockchain ha creato nuove sfide e opportunità per i criminali.

6.1 Banche digitali e denaro virtuale

Nel digital banking, quando il cliente si collega al server web della banca con il suo codice identificativo personale, poi inserisce la sua password personale e il sistema verificherà automaticamente la persona. Con questo sistema, usando una tecnica di phishing, i criminali possono effettuare transazioni senza recarsi in banca e senza compilare fisicamente numerosi moduli, rendendo il loro lavoro molto più semplice. A causa di questo accesso, non possono verificare l'identità individuale che accede effettivamente al conto dell'istituto finanziario. Inoltre, poiché i criminali finanziari possono intraprendere questa azione ovunque nel mondo e poiché non si sono recati fisicamente in banca, è meno probabile che vengano osservati. Pertanto, i criminali finanziari avranno accesso online e controllo sui propri conti bancari, indipendentemente dal luogo in cui si trovano. Inoltre, è più difficile determinare le attività svolte con e-cash o contante elettronico rispetto alle attività di riciclaggio di denaro reale. Ecco perché oggi

CamminoDiritto.it
ISSN 2421-7123

i criminali finanziari preferiscono svolgere attività basate sulla moneta elettronica piuttosto che sul denaro fisico.

6.2 Marketplace e E-commerce

I progressi tecnologici nel commercio elettronico hanno reso facile creare attività online e nasconderle dietro siti web di negozi legittimi. Pertanto, i riciclatori di denaro hanno iniziato a utilizzare i siti di e-commerce per sfruttare questa vulnerabilità e continuare le loro attività. In generale, i crimini finanziari che utilizzano questi percorsi sono chiamati riciclaggio di transazioni, che può essere descritto come riciclaggio di denaro nell'era digitale. I riciclatori di transazioni possono connettersi alle reti estese di siti web di commercio elettronico non dichiarati, riservati e illegali, nonché alle reti di pagamento dei fornitori di servizi. I fornitori di servizi commerciali sono tenuti a garantire che i siti web di e-commerce siano legittimi perché organizzazioni online inspiegabili possono facilmente infiltrarsi nei sistemi di pagamento attraverso il riciclaggio di pagamenti. Per evitare rischi e responsabilità associati alla facilitazione del riciclaggio delle transazioni, i processori di pagamento devono adottare una tecnologia avanzata di cyber intelligence che riveli reti di e-commerce, fornitori e attività correlate nascoste.

6.3 Casinò online

Esistono siti di gioco d'azzardo online registrati e siti di gioco d'azzardo online che non sono legalmente registrati. Poiché questi siti di gioco d'azzardo non sono registrati, non possono essere controllati dalle autorità di regolamentazione e le loro attività non possono essere monitorate. Un metodo frequente è dato da un gioco in cui uno o più giocatori perdono intenzionalmente contro un altro o trasferiscono tutte le loro fiches a un singolo giocatore. Quindi, quando un giocatore ottiene tutte le fiches, può guadagnare denaro e il denaro giocato da tutti i giocatori diventa denaro pulito.

6.4 Giochi online

Lo sviluppo dell'industria dei videogiochi ha comportato anche un aumento del rischio di riciclaggio di denaro. A causa della mancanza di normative in questo settore, questo settore è diventato un potenziale bersaglio per il riciclaggio di denaro. I riciclatori di denaro acquistano inventario di gioco con carte di credito illegali e poi vendono questo inventario a un prezzo inferiore rispetto al mercato nero. Pertanto, lavano il denaro nero che hanno e lo trasformano in denaro pulito.

6.5 Utilizzo dei social

CamminoDiritto.it
ISSN 2421-7123

Al giorno d'oggi le persone trascorrono sempre più tempo sui social media e quindi anche i reati finanziari che utilizzano i canali dei social media. I riciclatori di denaro possono creare programmi o identità false per fare denaro attraverso i social media e cercare di coinvolgere le persone in questi programmi. Perciò i riciclatori di denaro utilizzano le persone che ritirano nelle loro reti per prelevare denaro dai loro conti. Ciò significa che i criminali finanziari utilizzano queste persone come portavalori e i criminali generalmente prendono di mira i giovani. I criminali scelgono un conto che non ha precedenti penali per ridurre la probabilità di essere scoperti. Il denaro da riciclare viene trasferito dal conto dell'affiliato al conto bancario di terzi tramite bonifico bancario e il denaro ricevuto viene convertito in contanti. Successivamente, questo denaro viene convertito in una valuta virtuale come Bitcoin. A causa delle transazioni complesse, questo processo di riciclaggio di denaro è difficile da intercettare.

7. Il Digital Market Act e il Digital Service Act a confronto

Il Digital Markets Act (DMA) e il Digital Services Act (DSA) sono stati formulati dall'Unione Europea come risposta alle sfide poste dal mondo digitale. Questi due quadri legislativi condividono l'obiettivo comune di regolamentare i mercati digitali, ma differiscono per portata, focus e impatto previsto. Il DMA affronta principalmente il predominio delle grandi aziende tecnologiche nel mercato dell'UE e il loro potenziale impatto sulla concorrenza (8). L'obiettivo è garantire una concorrenza leale e pari opportunità per tutti gli attori del mercato digitale. Il DSA, invece, si concentra sulla responsabilità delle piattaforme online e mira a creare regole chiare e trasparenti per i fornitori di servizi digitali (9). I due strumenti vogliono proteggere gli utenti da contenuti dannosi, garantendo la loro sicurezza online. Le norme rientrino nell'ambito della strategia digitale dell'UE, il quadro normativo e l'autorità legislativa che esercitano differiscono in modo significativo. Il DSA, nel suo quadro di due diligence, sottolinea la protezione dei dati personali e della privacy degli utenti come componenti integranti della creazione di un ambiente digitale sicuro. Pur riconoscendo l'importanza dei dati personali, il DMA pone un'attenzione maggiore sulle questioni legate alla concorrenza, come garantire un accesso equo ai dati e prevenire lo sfruttamento del potere di mercato da parte dei gatekeeper. Per quanto riguarda gli obblighi imposti alle imprese, il DSA introduce obblighi ai fornitori di servizi di adottare misure per affrontare i rischi associati ai loro servizi. Ciò include misure proattive per contrastare la diffusione di contenuti illegali, contenuti violenti, proteggere i minori online e garantire l'integrità dell'ambiente online. Il DMA si concentra sui gatekeeper, imponendo obblighi più severi alle piattaforme online con un impatto significativo sul mercato interno: si appoggia al diritto della concorrenza commerciale, mirando a prevenire pratiche sleali da parte delle piattaforme digitali che detengono una quota di mercato rilevante. L'impatto del DSA e del DMA sui modelli di business e sulla trasformazione digitale è significativo: il DSA

CamminoDiritto.it
ISSN 2421-7123

incoraggia un modello di business responsabile che dà priorità alla sicurezza degli utenti e al rispetto delle normative. Al contrario, l'attenzione del DMA sulla concorrenza e sulle dinamiche del mercato mira a promuovere l'innovazione e la trasformazione digitale prevenendo pratiche anticoncorrenziali e garantendo condizioni di parità per tutte le aziende digitali.

8. Conclusioni

Per le istituzioni finanziarie, garantire gli ecosistemi digitali è vitale. Nel contesto economico più ampio, si registrano crescenti disuguaglianze tra le organizzazioni cyber-resilienti e quelle che non lo sono. Mentre le grandi organizzazioni hanno dimostrato miglioramenti in termini di sicurezza informatica, la resilienza informatica delle piccole e medie imprese (PMI) è in calo, nonostante costituiscano la maggioranza delle aziende in molti paesi del mondo. Inoltre, il rapporto del Forum ha rilevato che la disparità tra chi ha e chi non ha la sicurezza informatica è esacerbata dalle tecnologie emergenti, con molte PMI lasciate indietro dallo sviluppo di tecnologie avanzate. Lo Strategic Cybersecurity Talent Framework, un white-paper del World Economic Forum (10), ha rilevato che gli sforzi per raggiungere gli obiettivi di cybersecurity sono ostacolati da una continua carenza di competenze. Esiste una carenza globale di 4 milioni di professionisti della sicurezza informatica, con più della metà delle organizzazioni pubbliche che indicano la mancanza di risorse e competenze come la sfida più grande per migliorare la resilienza informatica.

CamminoDiritto.it
ISSN 2421-7123

Note e riferimenti bibliografici

Note e riferimenti bibliografici:

1. ISO/IEC 27001:2022 {https/URL}

2. “Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno” {https/URL}

3. Report “Reimagining the Future of Finance”, Boston Consulting Group, {https/URL}

4. Report “The Global Cyber Threat”, International Monetary Found, www.imf.org

5. Report “2022 Internet Crime Report”, FBI-Internet Crime Complaint Center, {https/URL}

6. “Questioni di Economia e Finanza” Banca di Italia, novembre 2024

7. Report “Opportunities and Challenges of New Technologies for AML/CFT” https://www.fatf-gafi.org, {https/URL}#160;https://digital-strategy.ec.europa.eu

8. Report “Strategic Cybersecurity Talent Framework”, World Economic Forum, www.weforum.org

* Il simbolo {https/URL} sostituisce i link visualizzabili sulla pagina:
https://rivista.camminodiritto.it/articolo.asp?id=10814