La Cybersecurity in azienda: minacce e presidi per dipendenti e cittadini

Incontro con Soci FederlegnoArredo

21 Aprile 2021

Agenda

- **Il contesto dei rischi cyber**
- Le principali tipologie di attacco e di frode nel contesto cyber
- Le best practice di sicurezza per le aziende
- I presidi di Intesa Sanpaolo a protezione della clientela

Grazie all'evoluzione tecnologica, la società sta affrontando un cambiamento radicale ricco di potenzialità…

Illustrativo

La *società tradizionale*…

Identità fisica

Oggetti fisici

Interazione di persona

Lavoro presso i locali aziendali

…è sempre più una *società digitale*

Identità digitale

Dati e asset virtuali

Interazione tramite social

Smart working

…ma anche di pericoli, spinti da digitalizzazione e Covid: cybercrime e frodi crescono esponenzialmente a livello globale

Principali driver di crescita

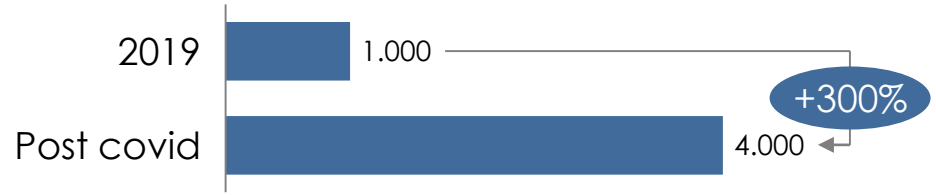
Significativo **incremento della rilevanza dei canali digitali** per le interazioni con la clientela e i **servizi pubblici e privati**

Estensione dei processi digitalizzati ed incremento delle interazioni digitali con le terze parti

Attacchi Cyber globali[4]

Frodi online globali

Segnalazioni giornaliere attacchi cyber all'FBI[1]
(#)



~6,2k

Numero attacchi cyber gravi con danni significativi[2] dal 2017 al 2020 (~400M$ per singolo attacco)

200B$

Perdite per **frodi** stimate **su pagamenti online** a livello globale tra il 2020 e il 2024[3]

1. Fonte: FBI Internet Crime Complaint Center, TheHill | 2. Rapporto Clusit 2021 sulla sicurezza ICT: riporta attacchi di particolare gravità (attacchi con impatto significativo per le vittime in termini di perdite economiche, di danni alla reputazione, di diffusione di dati sensibili o che comunque prefigurano scenari particolarmente preoccupanti) | 3. Juniper Research – Marzo 2020 | 4. 30% degli attacchi basati su ransomware con incremento richieste di riscatto

In particolare, le minacce cyber stanno aumentando principalmente in tre macro ambiti…

Macro ambiti di rischio	Descrizione del contesto esterno
1  Frodi ai danni di individui e aziende	**Attività finalizzate all'appropriazione illecita di denaro** alimentate principalmente da: • Campagne phishing, rese più efficaci grazie a nuove tecniche di *Swap SIM, Spoofing* e *Swap ALIAS*[1] , finalizzate all' indirizzamento verso siti web fraudolenti per appropriazione delle credenziali • Diffusione di malware (es. finalizzati alla sostituzione fraudolenta dell'IBAN beneficiario)
2  Attacchi alle infrastrutture aziendali	**Attacchi diretti alle infrastrutture** (es. infezioni Ransomware[2] e attacchi DDoS[3]) che comportano indisponibilità dei dati e dei sistemi aziendali, finalizzati alla richiesta di riscatti o al furto di dati e che possono comportare impatti significativi, tra cui anche il blocco dei servizi alla clientela
3  Attacchi "geopolitici", anche a terze parti	**Attacchi cyber condotti tra Stati** (e.g. Cina, Russia, Corea del Nord, Stati Uniti) a seguito delle recenti tensioni geopolitiche internazionali, finalizzati all'acquisizione di informazioni utili allo spionaggio ed al sabotaggio internazionale, con impatti su: • Attacchi alle aziende del settore privato che detengono infrastrutture strategiche (es. telco, operatori energetici) con **ripercussioni indirette anche su piccole e medie imprese** • Coinvolgimento collaterale in caso di **presenza nel paese oggetto di attacco**

Dettaglio del documento

1. Tecniche finalizzate ad appropriazione del telefono che autorizza l'accesso ai servizi digitali del cliente o alla falsificazione del mittente di una comunicazione via telefono, sms o mail; 2. Virus informatici che rendono inaccessibili i dati del sistema infettato con l'obiettivo di ottenere il pagamento di un riscatto; 3. Distributed Denial of Service, inondazione di richieste di accesso da fonti multiple a sistemi finalizzate alla saturazione della banda di comunicazione degli stessi

…per questo è importante imparare ad avere maggiore consapevolezza e responsabilità sul tema

Singolo individuo

Proteggere i propri dati e asset virtuali (es. non utilizzare stesse credenziali su siti diversi) e gestire le proprie relazioni digitali in sicurezza (es. Social Media)

Dipendente

Proteggere i dati e gli asset virtuali **dell'azienda,** adottando comportamenti cyber-safe

E' quindi fondamentale **apprendere la cybersecurity e metterla in pratica**, su tutti e 2 i livelli

Agenda

- Il contesto dei rischi cyber
- **Le principali tipologie di attacco e di frode nel contesto cyber**
- Le best practice di sicurezza per le aziende
- I presidi di Intesa Sanpaolo a protezione della clientela

Due principali elementi sfruttati dai cyber-criminali per compiere attacchi e frodi

Fattore umano

sfruttamento del comportamento umano con l'obiettivo di indurre un individuo a compiere una determinata azione

Vulnerabilità tecniche

sfruttamento delle vulnerabilità intrinseche dei sistemi e di un'eventuale scarsa protezione

Il 90%[1] degli incidenti cyber è innescato dal fattore umano a causa di comportamenti inadeguati…

Il **90%**[1] di tutti gli incidenti di sicurezza deriva da una qualche forma di **errore umano**…

Click su link malevoli e cessione delle credenziali

Utilizzo credenziali aziendali per attività personali (es. registrarsi a siti web o social network)

Navigazione su **siti web malevoli e connessione a reti poco sicure**

Gestione scorretta dei **dispositivi** (e.g. smarrimento, compromissione,…) e **disattenzioni durante la condivisione** di dati e informazioni

…con **potenziali impatti significativi sull'azienda**, diretti ed indiretti

Impatti **economici diretti**

Specifico per alcuni settori (es. Manufacturing)

Impatti sulla **sicurezza fisica del personale**

Impatti **normativi** / **sanzionatori**

Discontinuità del **business**

Impatti **reputazionali**

Necessità azioni di remediation all'incidente

INTESA SANPAOLO

1. IBM Cybersecurity Intelligence Index

…con alla base uno dei più grandi pericoli: il phishing in tutte le sue forme!

Phishing

Truffa effettuata su Internet attraverso la quale **un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali**, dati finanziari o codici di accesso, **fingendosi un ente affidabile** in una comunicazione digitale

E-mail phishing

Invio di una **e-mail** per fingersi un ente / persona affidabile

Smishing

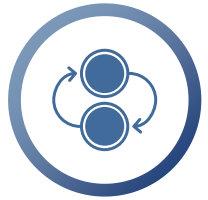
Invio di un **SMS** per fingersi un ente / persona affidabile

Vishing

Telefonata per fingersi un ente / persona affidabile

Swap ALIAS

La **fiducia della vittima** viene conquistata **camuffando il mittente**



Spoofing

La **fiducia della vittima** viene conquistata **camuffando il numero di telefono**

I frodatori utilizzano varie tecniche combinate (es. Swap ALIAS, Spoofing) **per fingersi entità / persone affidabili** e far "abboccare" le vittime

Inoltre, sono disponibili strumenti sempre più economici e semplici da reperire che «avvicinano» a noi i cyber attacchi

Strumenti gratuiti reperibili sul web

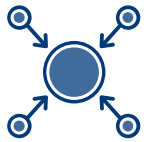
Prezzi medi attacchi/tool in vendita sul web

- Falsificazione del numero di telefono: gratis o ~1$
- Pagina di phishing pronta all'uso: ~3$
- Fac-simile di documenti falsificati[1]: ~17$
- Lista 600k indirizzi e-mail: ~10$
- Account di posta compromessi: ~80$

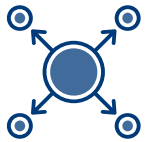
1. Layout contraffatto di documenti bancari, bollette,…

Anche le vulnerabilità di sistemi, reti e dati, se non gestite adeguatamente, possono «aprire le porte» agli attaccanti

Possibili vulnerabilità ICT



Rete e sistemi IT aziendali (es. sistemi ERP, sistemi IT centrali, etc.)



Rete e sistemi legati al monitoraggio / controllo della catena produttiva (i.e. Industrial Control Systems) **anche a livello di singolo sito** (es. sensori, RTU[1], GUI[2] per operare sui singoli componenti, etc.)

Sistemi gestiti da terze parti sia a livello centrale che a livello di catena produttiva

Dati memorizzati e scambiati su sistemi sia interni che esterni all'azienda (es. Cloud)

Illustrativo

Implicazioni

E' dunque necessario **proteggere e governare reti, sistemi e dati**:

- Centralmente e su tutta la catena produttiva **fino al livello di singolo componente**
- **Sia su sistemi interni che esterni** all'azienda (es. Cloud)

1. Remote Terminal Unit | 2. Graphical User Interface

Le principali tipologie di attacchi e frodi fanno leva su fattore umano o vulnerabilità tecniche

	Descrizione		Principali tipologie	Innesco
Frodi	**Non compromettono i sistemi e fanno leva principalmente sui comportamenti** degli individui (fattore umano)		1 **Phishing:** furto dei dati di accesso ai servizi digitali (es. conto corrente) e di eventuali ulteriori fattori di autenticazione tramite tecniche di social engineering	Fattore umano
			2 **CEO Fraud:** richiesta di pagamento fingendosi il CEO / un manager aziendale	Fattore umano
			3 **Invoice fraud:** richiesta di pagamento fingendosi un fornitore dell'azienda	Fattore umano
		Può essere usato anche come vettore di attacco (es. innestando un malware nel dispositivo della vittima)	4 **Help desk support:** furto di informazioni fingendosi il supporto tecnico di un azienda / software house e facendo installare alla vittima un software di controllo remoto	Fattore umano
Attacchi	**Compromettono i sistemi** (es. dispositivi, reti, servizi) e possono essere innescati tramite **fattore umano e/o sfruttando le vulnerabilità tecniche**		5 **Ransomware:** richiesta di un riscatto dopo aver crittografato dati e dispositivi su una rete tramite malware	Fattore umano Vulnerabilità tecniche
			6 **Man-in-the-Middle / Browser:** furto di informazioni intercettando una comunicazione tra due parti (es. intercettando le informazioni scambiate sulla rete wi-fi o tramite malware installato nel browser)	Fattore umano Vulnerabilità tecniche
			7 **Denial of Service (DoS):** rallentamento / blocco di un servizio tramite l'invio di dati ad-hoc che causano errori o di grandi moli di dati	Vulnerabilità tecniche
			8 **Advanced Persistent Threats (APT):** furto di informazioni a valle di un' intrusione e movimento laterale sui sistemi aziendali per lunghi periodi di tempo	Fattore umano Vulnerabilità tecniche

Principali golden rules per prevenire attacchi e frodi

Prevenzione attacchi
Prevenzione frodi

- **Non cliccare link e/o scaricare allegati da e-mail o SMS** se non si è certi dell'identità del mittente
- **Non condividere le informazioni dell'azienda al di fuori di essa** (e.g. organigramma, processi)
- Porre **attenzione durante la navigazione web** e scaricare solo software consentito
- Non utilizzare **indirizzi e-mail / le credenziali aziendali** per **registrarsi ai servizi web** (es. Social)
- **Rispettare le procedure aziendali in merito alla gestione dei pagamenti;** per richieste di pagamento al di fuori delle procedure rivolgersi a colleghi più esperti
- **Custodire ed utilizzare i propri dispositivi aziendali in sicurezza** evitando di cederli a terzi
- Effettuare **aggiornamenti periodici dei sistemi IT**
- Effettuare dei **test periodici di sicurezza per rintracciare eventuali vulnerabilità** (es. Vulnerability Assessment)
- Adottare soluzioni organizzative e tecnologiche per la **protezione dei dati** (es. crittografia) e la **gestione di accessi** e privilegi
- Adottare soluzioni organizzative e tecnologiche per la **protezione dei device** (es. smartphone, laptop)

Agenda

- Il contesto dei rischi cyber
- Le principali tipologie di attacco e di frode nel contesto cyber
- **Le best practice di sicurezza per le aziende**
- I presidi di Intesa Sanpaolo a protezione della clientela

Le aziende per gestire la cybersecurity dovrebbero dotarsi di un framework, composto da tre elementi principali

Governance

- Definire gli obiettivi e guidare la strategia di Cybersecurity coordinando i vari stakeholders coinvolti

Necessario per realtà con una spinta maturità IT

1

Persone e organizzazione

- Definire le strutture di cybersecurity delimitando specifici ruoli, responsabilità e relative interazioni
- Assumere persone competenti con skill diversificate (non solo tecnologiche)
- Limitare l'accesso alle informazioni in funzione del ruolo

2

Processi

- Definire e disegnare i processi operativi ed il framework di procedure interne a supporto delle attività di cybersecurity

3

Strumenti

- Adottare soluzioni tecnologiche e servizi per l'implementazione dei processi e la gestione delle attività di cybersecurity

I processi descrivono le modalità organizzative di presidio della cybersecurity

Illustrativo

Grado di maturità in ambito IT

Processo	Descrizione
Awareness	Aumento del **livello di consapevolezza** circa la rilevanza e pervasività del rischio cyber su tutti gli stakeholders coinvolti (es. dipendenti, clienti, fornitori,…)
Sicurezza degli accessi	**Potenziamento dei livelli di sicurezza durante gli accessi** e revisione periodica delle utenze e dei relativi privilegi
Sicurezza delle terze parti	**Classificazione, valutazione e monitoraggio dei fornitori** in termini di rischiosità (presidi cyber in essere del fornitore) e rilevanza (impatto potenziale di un attacco sul fornitore)
Cybersecurity by design	Sviluppo di **sistemi e applicazioni intrinsecamente sicuri** e conformi alla normativa e agli standard internazionali
Gestione delle vulnerabilità e patch management	Identificazione, classificazione, verifica, mitigazione e gestione delle **vulnerabilità tecniche legate agli asset informatici**
Presidio della normativa	**Adeguamento delle procedure interne** di cybersecurity all'evoluzione della tecnologia e degli standard di settore
Gestione degli incidenti di natura informativa	Gestione degli eventi di sicurezza a partire dalla **classificazione** fino all' **implementazione** di adeguate contromisure

Disponibili numerosi strumenti in commercio per la gestione a 360 gradi della cybersecurity

Illustrativo

☆ Particolarmente rilevanti in ambito Smart Working

Grado di maturità in ambito IT

Soluzione	Descrizione	Principali Funzionalità
Identity Management & Governance	Soluzioni per la gestione del ciclo di vita delle identità digitali e la verifica dei ruoli e dei privilegi di accesso degli utenti	• User provisioning • Gestione workflow approvativi
Access Control	Soluzioni per la gestione degli accessi ai sistemi e alle applicazioni	• Autenticazione • Autorizzazione • Single Sign-On
Multi-Factor Authentication ☆	Soluzioni per la gestione dell'autenticazione dell'utente, attraverso l'utilizzo di password dinamiche (One Time Password - OTP)	• Autenticazione
Virtual Private Network ☆	Soluzioni per il collegamento protetto e gli accessi dall'esterno al sistema informativo aziendale	• Data encryption • Accesso remoto
Secure Web Gateway	Soluzioni per la protezione della navigazione internet	• URL category filtering • URL reputation filtering • SSL inspection
Secure Email Gateway	Soluzioni per la protezione della posta elettronica	• Anti-spam /Anti-malware • Anti-phishing • Content / Attachment filtering
Data Protection / Data Loss Prevention	Soluzioni in grado di rilevare potenziali fuoriuscite di dati (data leakage) mediante il monitoraggio, la protezione e il blocco di dati considerati sensibili	• Data Classification • Content Aware Protection
Vulnerability e patch management	Soluzioni per l'identificazione, la classificazione e la mitigazione delle vulnerabilità relative ai sistemi e alle applicazioni e relative azioni di remediation	• Vulnerability discovery • Penetration tests
Protezione infrastrutture	Soluzioni per la protezione di pc, laptop e server	• Anti-virus, Anti-malware fino alle più evolute soluzioni di EDR[1] • Encryption • Web reputation • Personal firewall • Whitelisting software

1. Endpoint Detection and Response

Agenda

- Il contesto dei rischi cyber
- Le principali tipologie di attacco e di frode nel contesto cyber
- Le best practice di sicurezza per le aziende
- **I presidi di Intesa Sanpaolo a protezione della clientela**

Intesa Sanpaolo protegge i propri Clienti su più fronti

1

Sensibilizzazione del Cliente

Sensibilizzazione al Cliente sulle principali tipologie di frode e come proteggersi, tramite vari canali

2

Transaction Monitoring

Garanzia di un presidio costante delle disposizioni ritenute sospette ed effettuate tramite le carte di pagamento e l' E-Banking

3

Strong Customer Authentication

Utilizzo di almeno due fattori di sicurezza (e.g. SMS, PIN, biometria…) per l'accesso al conto e l'autorizzazione delle transazioni online

4

Tecnologie innovative

Utilizzo di tecnologie innovative e sofisticate come ulteriore strumento di protezione della clientela

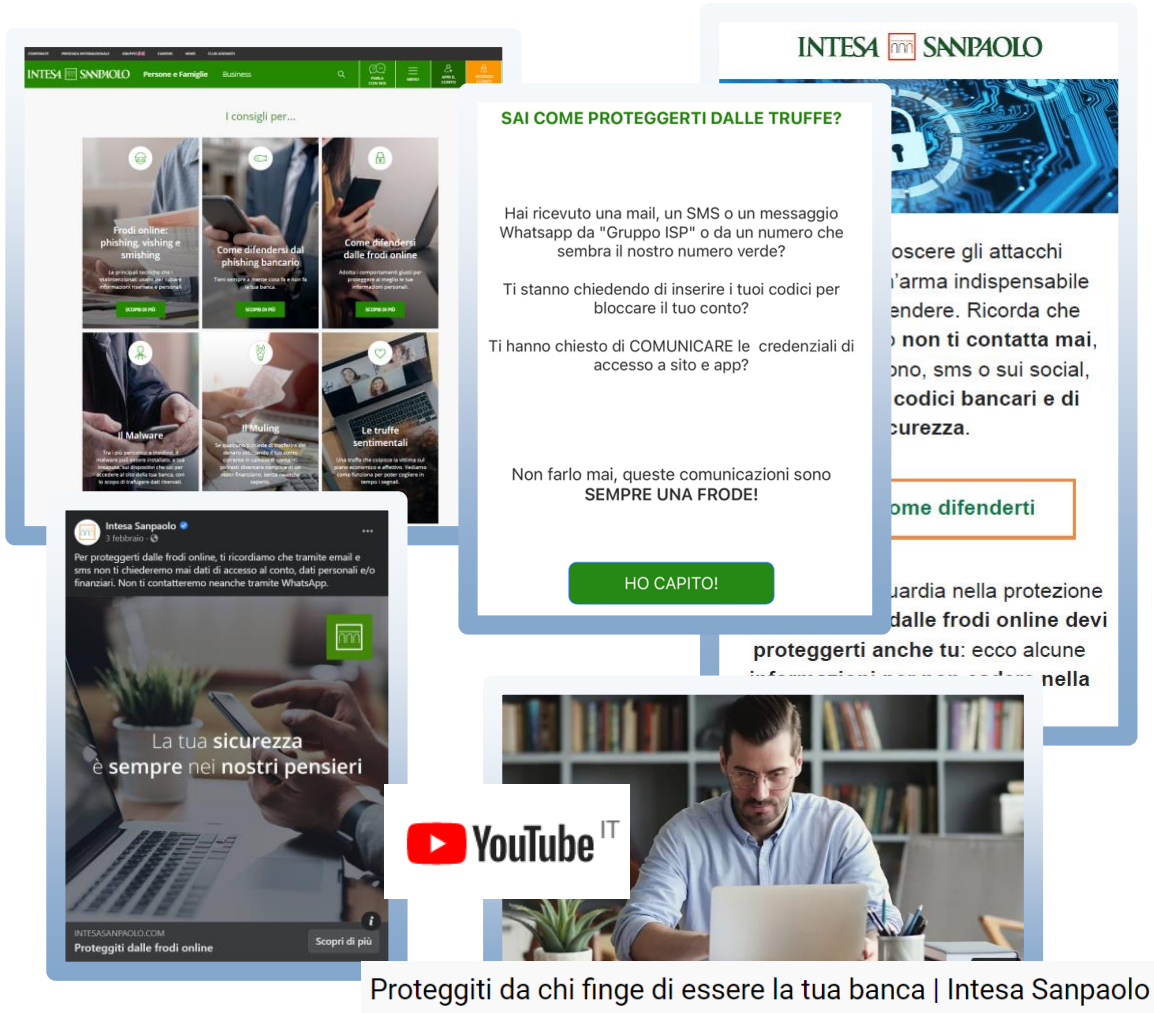
Inoltre, **Intesa Sanpaolo effettua una continua ricerca**, tramite fonti interne ed esterne, **per prevenire nuove tipologie di attacchi e frodi** anticipando i nuovi trend

La sensibilizzazione del Cliente avviene tramite vari canali

Principali canali / iniziative

- Presenza sezione di sicurezza sul sito di **internet banking**[1], sia retail che corporate
- Invio di **notifiche push / pop-up di sicurezza tramite app mobile**
- Invio di **Digital E-mail Marketing**
- Lancio di varie **campagne Social**
- Pubblicazione di una **videoguida su Youtube**[2]
- Sensibilizzazione tramite messaggi pre-registrati via **IVR**[3]

Esempi



Proteggiti da chi finge di essere la tua banca | Intesa Sanpaolo

1. https://www.intesasanpaolo.com/it/common/landing/anti-phishing.html | 2. https://www.youtube.com/watch?v=WAYTGnJaOEs | 3. Interactive Voice Response

La Strong Customer Authentication protegge l'accesso ai servizi digitali e l'operatività remota dei Clienti

Strong Customer Authentication
doppio livello di protezione per l'accesso al conto e l'autorizzazione delle transazioni

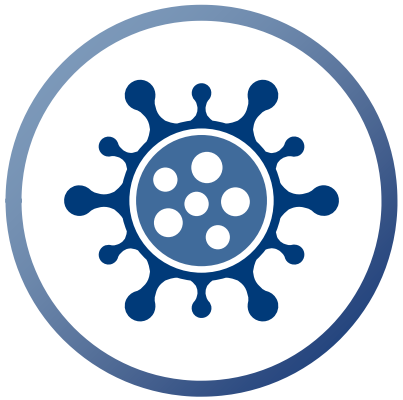
- Utilizzo combinato di **password statiche** (il Codice Titolare e il PIN) con una **password dinamica** (il codice O-Key), che si può utilizzare una volta sola per una singola operazione
- Il Codice O-Key può essere **ricevuto via SMS o generato dall'App** Intesa Sanpaolo Mobile in modo automatico
- **In entrambi i casi le notifiche (Push o SMS)** sul device indicano esattamente cosa si sta autorizzando
- Se supportate dal Device, è possibile autorizzare con le **grandezze biometriche** (es. impronta, riconoscimento facciale, iride..)
- Possibile utilizzo anche di **dispositivi fisici OTC**[1] (dedicato al mondo corporate)

Codici SMS in progressiva dismissione per limitare le informazioni comunicabili ai frodatori

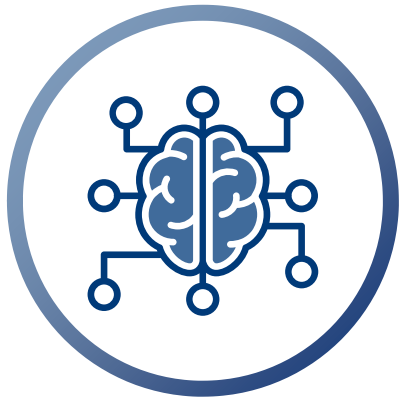
1. Token con lettore QR code per la generazione di password temporanee

Intesa Sanpaolo adotta anche tecnologie innovative e sofisticate, in aggiunta agli altri livelli di protezione

Certificazione dei dispositivi del Cliente utilizzati per i servizi bancari e progressiva **eliminazione dei codici di sicurezza SMS** comunicabili ai frodatori



Utilizzo di **nuovi strumenti di verifica dell'integrità dei dispositivi** della clientela (es. Malware Detection, SIM Swap)



Piattaforme evolute che permettono di utilizzare i dati relativi all'operatività bancaria usuale dei clienti[1] (es. regole profilate per cliente) per mettere in sicurezza le transazioni potenzialmente rischiose

1. Customer Behavior Monitoring

Grazie

Dott. Ugoste Fabio

Head of Cybersecurity and Business Continuity Management, Information Security Officer del Gruppo Intesa Sanpaolo