BANCA D'ITALIA
EUROSISTEMA

IVASS
ISTITUTO PER LA VIGILANZA SULLE ASSICURAZIONI

Note Covid-19 - 17 aprile 2020

LA SICUREZZA CIBERNETICA AI TEMPI DEL COVID-19

GRUPPO DI COORDINAMENTO PER LA SICUREZZA CIBERNETICA BANCA D'ITALIA-IVASS

L'epidemia Covid-19 accelera il processo di digitalizzazione, introducendo nuovi rischi cibernetici. La Banca d'Italia e l'IVASS rafforzano la protezione dei sistemi informatici interni e, nell'ambito delle competenze istituzionali, contribuiscono a garantire la sicurezza del sistema finanziario e assicurativo. Rinnovano inoltre l'impegno a tutela degli utenti di servizi finanziari digitali, con particolare attenzione alle persone e alle imprese che prima dell'epidemia facevano ricorso alla rete in misura modesta.

La pandemia di Covid-19 sta accelerando la digitalizzazione delle economie. Per combattere il contagio è necessario il distanziamento sociale: la scuola, il lavoro e la socialità si spostano *online*; cresce la fruizione di servizi in modalità remota, anche in campo bancario e assicurativo.

Questa trasformazione rimarrà a emergenza finita, con effetti positivi: più digitalizzazione può significare più produttività, meno inquinamento, più agevole conciliazione tra vita e lavoro. Aumenta contestualmente il rischio di attacchi informatici. Sono particolarmente esposte le persone e le imprese che in passato facevano ricorso alla rete in misura modesta e non sempre sono consapevoli delle insidie del mondo digitale.

La Banca d'Italia da tempo è in prima linea nel contrasto alla minaccia cibernetica. Essa opera per rafforzare la propria sicurezza informatica (in quanto infrastruttura critica, erogatrice di servizi digitali e custode di dati sensibili), e quella del sistema finanziario, in qualità di autorità di supervisione dei sistemi di pagamento e di altre infrastrutture di mercato, nonché di autorità di vigilanza bancaria e finanziaria.

L'IVASS utilizza i servizi informatici e i presidi di sicurezza della Banca e, in qualità di autorità di vigilanza sul sistema assicurativo, opera per monitorarne e rafforzarne la sicurezza informatica[1].

La Banca d'Italia e l'IVASS operano mediante:

[1] Per un approfondimento si veda Gruppo di Coordinamento per la Sicurezza Cibernetica, "Sicurezza cibernetica: il contributo della Banca d'Italia e dell'IVASS", Tematiche Istituzionali, Banca d'Italia.

– la costituzione di adeguati presidi difensivi interni, che includono il *Computer Emergency Response Team* (CERT) della Banca (CERTBI) particolarmente impegnato nella raccolta di informazioni sulle vulnerabilità e sugli incidenti informatici;

– la partecipazione a tavoli tecnici internazionali ed europei delle banche centrali e del settore finanziario, per la definizione di linee guida sulla sicurezza e l'incident reporting nonché lo sviluppo di test europei sulla resilienza cyber delle infrastrutture e dei principali operatori;

– l'emanazione di regolamentazione nazionale per rafforzare la *governance* dei processi informatici e i presidi in materia di sicurezza cibernetica;

– la vigilanza e la supervisione delle infrastrutture di mercato e degli operatori finanziari nazionali, anche attraverso ispezioni, la valutazione dei piani strategici e la predisposizione di strumenti di autovalutazione;

– lo scambio di informazioni e di ricerche con le altre istituzioni impegnate sul fronte della difesa da attacchi cibernetici;

– lo stimolo alla cooperazione pubblico-privato per la condivisione delle informazioni e per la creazione di capacità difensive, anche attraverso la gestione del CERT del settore finanziario italiano (CERTFin), in collaborazione con l'Associazione bancaria italiana (ABI) e con la partecipazione delle maggiori imprese bancarie e assicurative;

– il rafforzamento, per mezzo dell'educazione finanziaria, della consapevolezza di giovani e adulti in merito all'utilizzo di servizi finanziari e assicurativi digitali;

– la raccolta e l'analisi di dati statistici sulla frequenza e sull'impatto economico degli attacchi informatici contro le aziende italiane;

– la valutazione delle azioni di mitigazione del rischio cibernetico, ad esempio, in ambito assicurativo le coperture tramite polizze dedicate (cyber insurance).

Le due istituzioni stanno affrontando con particolare attenzione le sfide poste dalla pandemia. Ad esempio, nelle ultime settimane criminali informatici hanno diffuso numerosi messaggi di posta elettronica fraudolenti che pubblicizzano sedicenti cure contro il Coronavirus o fittizie iniziative di solidarietà, nel tentativo di sottrarre ai destinatari somme di denaro e credenziali di accesso ai conti *online* (c.d. *phishing*). La circolazione di questi messaggi contribuisce anche a generare confusione nel pubblico. Non sono nemmeno mancati gli attacchi contro le infrastrutture informatiche ospedaliere, in Italia come in altri Paesi.

Il CERTBI del Dipartimento Informatica conduce, in aggiunta all'attività ordinaria, approfondimenti mirati sulle caratteristiche di queste minacce (*cyber threat intelligence*), anche sulla base della continua condivisione di informazioni con controparti fidate e *partner* tecnologici (*infosharing*). Si concentra inoltre sulle vulnerabilità derivanti dal più intenso ricorso al telelavoro. È impegnato in interventi di innalzamento della consapevolezza del rischio (*security awareness*) in favore del personale della Banca e dell'IVASS e, in collaborazione con le unità dedicate alla Tutela della clientela ed educazione finanziaria, della cittadinanza nel suo complesso. In quest'ultimo ambito sono in preparazione nuovi materiali illustrativi sui comportamenti da tenere per fruire in sicurezza del *mobile banking* e di altri servizi finanziari digitali, a partire proprio dalla difesa contro il *phishing*.

Il CERTFin, in collaborazione con altre istituzioni, sta contribuendo da parte sua a irrobustire le difese del sistema finanziario nazionale. Gli strumenti comprendono l'*infosharing* tra intermediari, la diffusione di bollettini di sicurezza, l'organizzazione di *webinar* sulle tecniche di attacco, le possibili contromisure da adottare, la formazione sul corretto utilizzo dei dispositivi aziendali e il rafforzamento dei presidi connessi al lavoro da remoto.