ACCORDO EX ART. 4, L. 300/1970

SSL Inspection

Il giorno 10 giugno 2020

tra

ING Bank NV – *Milan Branch* rappresentata da Silvia Cassano, Andrea Chiesa e Alice Marini (di seguito anche la "**Banca**" o "**ING**")

e

le **Organizzazioni Sindacali** rappresentate dalle rispettive RSA (di seguito anche le "**OOSS**" e, congiuntamente alla Banca, le "**Parti**")

FABI

FIRST CISL

FISAC CGIL

UILCA

UNISIN

Premesso che

- l'esperienza recente dimostra l'evolversi di forme sempre più insidiose di *CyberCrime* e il crescente rischio di importazione nelle reti aziendali, attraverso la navigazione *Internet* anche mediante l'accesso a siti crittografati (https), di materiale informatico dannoso, quali *virus*, *malware*, etc.;

- in particolare, l'importazione di contenuti malevoli presenta rilevanti profili di potenziale pericolo in considerazione della metodologia applicata nella diffusione di *malware* e *virus*, che si inseriscono nelle reti aziendali al fine di esportare informazioni e dati di valore, o semplicemente di danneggiare sistemi e applicazioni, manifestando i propri effetti o potendo essere individuati anche molto tempo dopo il *download*;

- il fenomeno di cui al punto che precede, dunque, pericoloso in generale per tutti i sistemi informatici, diviene nel settore bancario ancora più insidioso e fonte di potenziali gravissimi danni, considerata la tipologia di dati custoditi nelle reti aziendali degli operatori del settore;

- quanto sopra rappresentato impone, dunque, alla Banca, nel rispetto delle *Policy* interne e di Gruppo, quale provvedimento imprescindibile a tutela della sicurezza dei propri sistemi, l'introduzione di misure più stringenti di controllo del traffico *Internet*;

- in questo contesto, la Banca ha dunque deciso di introdurre il controllo sul traffico *Internet* crittografato (siti https) dei dipendenti (di seguito anche "***SSL Inspection***"), con riferimento agli accessi alla rete effettuati utilizzando gli strumenti di lavoro in dotazione (PC, *tablet*, *smartphone*);

- il sistema *SSL Inspection* è volto ad analizzare se i *file* scaricati o le URL visitate contengano materiale dannoso quali *virus*, *malware*, etc., che possano rappresentare una potenziale compromissione dell'ambiente informatico ed è dunque determinato da esclusive ragioni di sicurezza del lavoro e di tutela del patrimonio informatico e informativo aziendale previste dall'art. 4, comma 1, della legge 20 maggio 1970, n. 300 (Statuto dei Lavoratori), non comportando alcuna forma di controllo a distanza e/o di monitoraggio dell'attività lavorativa, né alcun controllo di contenuti sul traffico *Internet* dei lavoratori;

- il trattamento dei dati personali avverrà in conformità alle vigenti disposizioni in materia;

- la Banca e le OOSS, condivise le esigenze di sicurezza e di tutela del patrimonio aziendale sopra descritte, anche nell'ottica di favorire la regolarità ed efficienza dello svolgimento delle attività lavorative, sottoscrivono il presente accordo ai sensi dell'art. 4, l. 300/1970 (di seguito anche l'"Accordo").

Tutto ciò premesso, le Parti convengono quanto segue.

1. **Premesse**

1.1. Le premesse formano parte integrante del presente Accordo.

2. **Il sistema *SSL Inspection*: definizione e finalità**

2.1. La Banca introdurrà a partire dal 15 giugno 2020 il controllo sul traffico *Internet* crittografato (siti https) dei dipendenti con riferimento agli accessi alla rete effettuati utilizzando gli strumenti di lavoro in dotazione (PC, *tablet*, *smartphone*), identificato come *SSL Inspection*, al fine di analizzare se i *file* scaricati o le URL visitate contengano materiale dannoso quali *virus*, *malware*, o altri contenuti malevoli che possano compromettere l'ambiente informatico.

2.2. Il sistema *SSL Inspection* è determinato da esclusive ragioni di sicurezza del lavoro e di tutela del patrimonio informatico e informativo aziendale previste dall'art. 4, comma 1, della legge 20 maggio 1970, n. 300 e non comporterà alcuna forma di controllo a distanza e/o di monitoraggio dell'attività lavorativa, né alcuna analisi dell'attività di navigazione del dipendente, lettura del contenuto dei siti visitati o degli eventuali documenti malevoli scaricati.

3. **Funzionamento del sistema *SSL Inspection***

3.1. Il traffico *Internet* crittografato viene suddiviso in quattro categorie di siti, in linea con le

policy di *Head Office* di ING per finalità di sicurezza IT e riferito a tutto il traffico *Internet*, crittografato e non:

- *blocked*, ovvero i siti rispetto ai quali è inibita la navigazione;
- *allowed*, ovvero i siti rispetto ai quali la navigazione è concessa senza controllo del traffico (a questa categoria appartengono, ad esempio, i siti delle banche, degli ospedali, delle assicurazioni, etc.). La Banca dichiara, in particolare, che il traffico da e verso siti Internet che trattano dati sanitari e/o finanziari non è soggetto a controllo nè ispezionato;
- *inspected*, ovvero i siti rispetto ai quali la navigazione è concessa con controllo del traffico (a questa categoria appartengono, ad esempio, i siti di dei giornali, etc.);
- *coached*, ovvero i siti rispetto ai quali la navigazione è concessa con controllo del traffico dopo un *warning message* automatico relativo ai rischi di perdita dei dati;

La collocazione dei siti *Internet* nell'una o nell'altra delle quattro categorie sopra indicate è stata effettuata sulla base di una astratta valutazione di "pericolosità" - quanto alla esclusiva possibilità di incappare in contenuti malevoli - determinata dalla materia trattata dai siti medesimi.

3.2. Il controllo viene effettuato sui siti crittografati *coached* e *inspected*.

3.3. Rispetto a queste ultime categorie di siti, la procedura di accesso a *Internet* e conseguentemente il controllo avviene attraverso i seguenti passaggi:

(i) la richiesta di accesso ad un determinato indirizzo https parte dal PC o altro dispositivo del dipendente e viene indirizzata a un *server* centrale di ING collocato, nelle sue varie dislocazioni, interamente nel territorio dell'Unione Europea (*proxy*);
(ii) il *proxy* trasmette la richiesta di accesso al sito selezionato dal dipendente;
(iii) nel caso in cui, attraverso l'accesso al sito, venga scaricato un contenuto "malevolo", il *proxy* invia un *alert* al GSOC (*Global Security Operation Center*), che ospita un altro server di proprietà ING che si trova in Polonia;
(iv) presso il GSOC viene effettuato un *triage* sul grado di gravità del *malware* scaricato;
(v) nei casi più gravi e potenzialmente tali da inficiare il funzionamento del sistema informatico italiano (al quale appartiene il dispositivo dal quale è partita la richiesta di accesso al sito), il GSOC trasmette un *alert* al dipartimento IT italiano, Area IT Security;
(vi) viene attivata a questo punto la procedura di gestione dell'incidente secondo la *Security Event Management Procedure* in vigore presso ING Bank N.V. – *Milan branch*.

3.4. L'indirizzamento del traffico *Internet* proveniente dall'Italia verso il *proxy* avviene attraverso la configurazione in tal senso del singolo dispositivo del lavoratore e non comporta l'installazione di alcun *software*.

3.5. Il sistema analizza il traffico "in transito": i dati di URL non vengono registrati, in modo tale da non tracciare nemmeno eventuali *user name* e *password* in essi presenti.

4. Tipologia di strumenti di lavoro soggetti a *SSL Inspection*

4.1. Gli strumenti di lavoro attraverso i quali potrà darsi luogo al controllo *SSL Inspection* sono il PC, lo *smartphone*, il *tablet*. Laddove la Banca dovesse mettere a disposizione per i

lavoratori eventuali altri dispositivi per lo svolgimento dell'attività lavorativa la Banca informerà preventivamente le OOSS prima di sottoporli al controllo SSL Inspection.

5. **Informazioni registrate, *audit trail* e conservazione**

5.1. Le informazioni di traffico che verranno registrate sono le seguenti:

- data e ora di connessione;
- utenza "corporate key";
- indirizzo IP;
- nome del dispositivo;
- indirizzo (URL) di connessione.

5.2. Nel caso si ravvisasse la necessità di registrare ulteriori tipologie di informazioni rispetto a quelle qui elencate, le integrazioni saranno oggetto di specifica e tempestiva informativa alle OOSS in apposito incontro ovvero a mezzo email, a seguito della quale le Parti valuteranno congiuntamente le eventuali necessità di modificare o integrare il presente Accordo.

5.3. Gli *audit trail* (ossia la cronologia della navigazione *Internet*) verranno conservati per sei mesi per finalità di verifica e ricostruzione dell'accaduto. Il tempo di conservazione è giustificato dalle particolari necessità di sicurezza di ING e dalla necessità di scoprire l'esistenza di *virus* o *malware*, alcuni dei quali si manifestano o possono comunque essere individuati anche molto tempo dopo il *download*.

5.4. Trascorso il periodo di conservazione come sopra indicato, i dati saranno cancellati e non potranno più essere utilizzati, ad eccezione dei casi in cui sia in corso su di essi una investigazione interna per la ricerca delle cause di un incidente o sia in corso un giudizio e salvo richiesta di conservazione oltre tale limite temporale da parte dell'Autorità Giudiziaria.

5.5. I *log* di navigazione verranno ricostruiti e analizzati solo in caso di incidente confermato da parte di personale autorizzato, addetto alle investigazioni e dotato delle necessarie competenze, facenti parte delle aree CISO - Chief Information Security Office (locale e globale), di IRM (Information risk Management) e di CIRM (Corporate Information Risk Management).

5.6. Gli addetti alle aree CISO e IRM locale potranno richiedere, a mezzo email, informazioni relativamente all'incidente, al dipendente che ha effettuato la navigazione Internet da cui è stato scaricato il contenuto malevolo che ha generato l'*alert*, i quali saranno tenuti a dare prontamente una risposta.

5.7. Nei casi in cui si rendessero necessari ulteriori chiarimenti e verifiche sui *log* di navigazione di cui al punto 5.5. che precede, potrà, inoltre, essere sentito nell'ambito di un incontro il dipendente interessato da parte degli addetti delle aree CISO e IRM locale, i quali potranno coinvolgere anche il Responsabile del dipendente. In questa sede il dipendente interessato

avrà la possibilità di richiedere l'assistenza di un rappresentante sindacale.

6. **Potere disciplinare**

6.1. A seguito della consultazione degli *audit trail* in caso di incidente, la Banca si impegna a non adottare verso i lavoratori interessati provvedimenti disciplinari, fatte salve le ipotesi di dolo e colpa grave. Quest'ultima dovrà comportare un danno oggettivo e non potenzale per la Banca e comunque una evidente negligenza del dipendente di cui si accerti la colpa. Sono escluse dalle ipotesi di colpa grave i casi in cui la navigazione internet da cui è scaturito il contenuto malevolo è avvenuta nel rispetto della policy sull'utilizzo degli strumenti elettronici aziendali ed è stata esclusivamente funzionale allo svolgimento dell'attività lavorativa.

7. **Informativa ai dipendenti e rispetto delle *Policy* esistenti**

7.1. La Banca si impegna ad informare i lavoratori in ordine al sistema *SSL Inspection* in tutte le sue implicazioni, anche attraverso la consegna a mezzo email di informative individuali redatte in conformità alla vigente normativa (in allegato il format dell'informativa individuale) e integrazioni della vigente *Policy sull'utilizzo degli strumenti elettronici aziendali* ove necessario.

7.2. La Banca e le OOSS si impegnano a sensibilizzare i dipendenti in merito al corretto uso degli strumenti informatici e al rispetto delle relative *policy* di tempo in tempo in vigore.

8. **Incontro di verifica**

8.1. Ogni anno le Parti effettueranno un incontro di verifica per valutare gli effetti dell'applicazione del presente Accordo.

Letto, firmato e sottoscritto.

ING Bank N.V. – Milan Branch

FABI

FIRST CISL

FISAC CGIL

UILCA

UNISIN