VERBALE DI ACCORDO IN MATERIA DI SICUREZZA CIBERNETICA

Siena, 25/09/2018

tra Banca MPS SpA
e le Segreterie degli Organi di Coordinamento delle RR.SS.AA

Premesso che

- Banca MPS è considerata infrastruttura sistemica nel panorama creditizio nazionale e sovranazionale e come tale è esposta al rischio attacchi informatici sempre più sofisticati;
- è obbligo dell'Azienda, come previsto anche dalla Direttiva UE 2016/1148 cui è stata data recente attuazione col decreto legislativo 18 maggio 2018, n. 65, in vigore dal 24 giugno 2018, adottare misure di sicurezza e di notifica degli incidenti con impatto rilevante per garantire un livello comune elevato di sicurezza delle reti e dei sistemi informativi;
- a tal fine, nell'ottica di creare una rete di protezione su più livelli dei propri sistemi informativi, Banca MPS nel mese di marzo 2018 ha sottoscritto una convenzione con la Polizia di Stato per avvalersi del supporto consulenziale, informatico e tecnico del Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC) all'interno del Servizio di Polizia Postale e delle Comunicazioni;

Considerato che

- l'Azienda per ottemperare ai predetti obblighi e garantire un elevato standard di protezione deve implementare il proprio presidio di sicurezza aziendale integrando gli attuali sistemi con una nuova soluzione di cyber security di protezione dalle minacce e di monitoraggio automatico del traffico dati;
- il sistema di cyber security adottato consente, infatti, il monitoraggio, con modalità automatiche, del traffico dati in entrata e in uscita dall'azienda in modo da rilevare eventi anomali e riconoscere, intercettare e bloccare i contenuti malevoli anche cifrati che rappresentino un rischio o possano veicolare una minaccia per le infrastrutture, il patrimonio e le informazioni dell'Azienda e dei suoi clienti;
- l'adozione del predetto sistema risponde esclusivamente ad esigenze di sicurezza del patrimonio aziendale - inteso sia come patrimonio economico ed informativo del Gruppo sia come informazioni che clienti, fornitori ed altre Istituzioni scambiano col Gruppo - e di prevenzione di frodi anche attraverso l'utilizzo di tecnologie informatiche;
- ai sensi dell'articolo 4, della legge 20 maggio 1970, n. 300 gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale;

tutto quanto sopra premesso e considerato
in relazione alle previsioni dell'art.4 della L. 300/70 le parti convengono quanto segue:

- i dati rilevati dal sistema di cyber security adottato, salvo quanto previsto dai successivi capoversi, saranno trattati per le sole finalità di sicurezza del patrimonio aziendale come sopra descritto, restando esclusa qualsiasi attività di monitoraggio dei lavoratori sia sotto il profilo quantitativo che qualitativo della prestazione lavorativa;
- gli eventi rilevati e classificati in modo automatico come anomali e/o potenziali incidenti di sicurezza saranno sottoposti ad analisi da parte delle competenti Funzioni di Sicurezza allo scopo sia di diagnosticare eventuali malfunzionamenti del sistema o falsi positivi che di fornire immediata assistenza agli utenti. Ove l'evento rappresenti, invece, una effettiva infrazione di sicurezza o un tentativo di frode, saranno adottate le opportune misure correttive e di contrasto volte ad isolare la problematica, a mitigarne gli effetti malevoli e contrastarne il ripetersi;
- i dati, compresi i log relativi alle anomalie riscontrate, saranno conservati in stretta osservanza delle norme previste dal Codice della Privacy e dalla normativa di riferimento tempo per tempo vigente;
- qualora l'analisi tecnica dell'anomalia renda opportuna la visualizzazione del traffico dati di una singola utenza, ciò potrà avvenire esclusivamente da parte di personale appartenente alle predette Funzioni di Sicurezza e delle Funzioni di Audit ed esclusivamente per le finalità di tutela del patrimonio dell'Azienda come sopra descritto, di prevenzione e contrasto alle frodi oltre che di supporto alla Magistratura e/o alle Forze dell'Ordine nella repressione di eventi criminosi, rimanendo escluso ogni utilizzo dei dati rilevati a fini disciplinari, fatti salvi i casi di dolo e colpa grave; in tali ultimi casi, il dipendente sarà informato dalle competenti funzioni delle Risorse Umane e potrà richiedere la visione degli elementi con facoltà di farsi assistere – conferendo apposito incarico in forma scritta – da un rappresentante aziendale delle Organizzazioni Sindacali firmatarie del presente accordo.
- l'andamento dell'utilizzo del sistema di cyber security adottato sarà oggetto di verifica congiunta a livello centrale a richiesta di una delle Parti.

Siena, 25/09/2018

L'Azienda Le OO.SS.