Verbale di accordo

In data 12 aprile 2021 presso la sede di via Rizzoli 8 a Milano, nonché a mezzo videoconferenza per i colleghi della RSA di Roma via Campania, si sono incontrati la Direzione aziendale di RCS MediaGroup e le RSU Quotidiani, RSU MediaGroup e RSA Roma di RCS:

Premesso che:

- La trasformazione digitale sta interessando ogni giorno di più i processi aziendali. Con la digitalizzazione anche il rischio delle minacce informatiche sta crescendo.
- Gli attacchi informatici continuano ad aumentare in frequenza, numerosità, velocità, sofisticazione e sono sempre più difficile da rilevare.
- RCS MediaGroup si trova a dover fronteggiare, come tutti i principali Gruppi Industriali in Italia e nel mondo, la continua escalation degli attacchi cyber che mirano a:
    - **sottrarre dati e documenti,**
    - **bloccare l'operatività delle società**, rendendo inaccessibili le informazioni presenti sui posti di lavoro e, più in generale, sull'infrastruttura informatica del Data Center (ad esempio: cifrando i dati presenti sui supporti di storage) e richiedere attività onerose e costose per ripristinare gli ambienti di lavoro e recuperare i dati/documenti sottratti.
- I sistemi di protezione tradizionali (es. antivirus), basati sulla conoscenza pregressa delle modalità di attacco, non sono più sufficienti per bloccare hacker che variano quotidianamente le tecniche di intrusione, riuscendo ad aggirare la protezione e distribuire il software malevolo ("malware"), in pochi secondi, sull'intera infrastruttura informatica del giornale e dell'azienda, creando importanti danni sia diretti che indiretti e arrivando nei casi più gravi a paralizzarne completamente l'attività.
- RCS, in ragione della propria attività, raccoglie e tratta dati riservati, anche sensibili. Tutti questi dati ricoprono rilevanza non solo per dipendenti, per i terzi e per la Società ma assumono anche una rilevanza pubblica.
- Inoltre, le obbligazioni di prevenzione e protezione contro i data breach imposte dal regolamento privacy impongono l'utilizzazione di adeguati strumenti tecnologici.
- Questo profilo di minaccia diversificato si è evoluto per includere un approccio di "minaccia mista" che combina attacchi esterni e minacce interne.
- La perdita dei dati può causare significativi danni economici, strategici e di immagine per l'Azienda.
- L'obiettivo di RCS è dotarsi di strumenti e procedure che possano fronteggiare l'aumento sia quantitativo sia qualitativo degli attacchi cyber limitando il più possibile i rischi per l'azienda e per i propri dipendenti. Nelle pagine seguenti sono descritte le azioni che RCS intende adottare:
    - Introduzione di nuovi strumenti a protezione dei dati e delle infrastrutture aziendali
    - Modifica delle policies e delle procedure di prevenzione e risposta
    - Un nuovo modello organizzativo dedicato alla Cybersecurity

- Le azioni relative ai software di protezione che RCS intende perseguire sono:
  - Potenziamento degli strumenti di email protection
  - Introduzione «nuovi strumenti» di End point Detection and Response («EDR»)
  - Introduzione di «nuovi strumenti» di correlazione e intelligenza artificiale («SIEM»)
- Dall'installazione e implementazione di tali Software deriva anche la possibilità preterintenzionale di controllo a distanza dell'attività dei lavoratori per le seguenti motivazioni:
  - Sicurezza sul lavoro, sicurezza dei dati e tutela del patrimonio aziendale.
- Tali Software sono residenti sui sistemi informativi centralizzati di proprietà o messi a disposizione del Gruppo RCS e per tale ragione:
  - è possibile condurre una verifica unitaria e centralizzata delle problematiche emergenti ai fini dell'applicazione della normativa citata;
  - è indispensabile prevedere una disciplina unitaria che regolamenti l'utilizzo di tali Software;
  - in ragione di quanto sopra si è proposta la necessità di trovare una intesa con le rappresentanze sindacali ai sensi di Legge.

Tutto ciò premesso le Parti concordano quanto segue:

a) i componenti delle RSU/RSA di RCS MediaGroup SpA sono i soggetti che costituiranno gli interlocutori di RCS legittimati a ricevere le informazioni e a partecipare ai controlli di seguito previsti. Per tale ragione, quando partecipano alle operazioni di gestione previste in questo accordo devono essere identificati, la loro partecipazione annotata nel processo verbale e sono tenuti ai doveri di riservatezza imposti dalla normativa sulla privacy agli incaricati del trattamento dei dati, oltre ai doveri specifici derivanti dall'acquisizione di informazioni riservate aziendali concernenti sistemi protetti dalle regole sulla proprietà intellettuale e che vengono qui identificate come informazioni segrete ai sensi dell'art. 98 della L.n. 30/2005, e dai doveri di riservatezza imposti dagli artt. 615 c.p. e seguenti, oltre specificamente da un impegno di riservatezza convenzionale, anche rafforzativo degli obblighi di cui all'art. 2105 c.c., secondo cui non potranno divulgare alcuna informazione sui contenuti e sulle notizie che abbiano acquisito in adempimento del loro incarico derivante dal presente accordo.

b) Tutti i dati delle persone che partecipano al procedimento di verifica restano riservati, tranne i casi di necessità per la tutela dei diritti (di RCS, dei partecipanti al procedimento, delle RSU/RSA quali soggetti firmatari del presente accordo).

c) I Software e i dati cui si riferisce la presente intesa sono quelli sinteticamente descritti in premessa nonché dettagliati specificamente nell'Allegato 1 al presente accordo, che ne costituisce parte integrante. RCS si impegna a fornire informazione preventiva di ogni richiesta o necessità di modifica dei medesimi così come della eventuale necessità della introduzione di nuovi SW che rivestano le caratteristiche di cui all'art. 4, co. 1 della Legge n°300/70.

d) Tale elenco contiene:
- le schede tecniche delle tecnologie installate (Allegato 1).

e) RCS si impegna a dare le informazioni di cui all'art. 13 del GDPR ai dipendenti e garantisce il rispetto delle normative di Legge sul trattamento dei dati quali risultano anche dal Codice Privacy come modificato dal D.Lgs.101/18,ai sensi del co. 3 dell'art. 4 Legge n°300/70.

f) I dati registrati dai Software sono trattati automaticamente in fase di screening e su base continuativa e anonima a fini preventivi; in caso di trattamento di dati individui è previsto l'intervento di team globali di specialisti per l'esclusione di falsi positivi funzionali alla prevenzione di ipotesi di accessi abusivi a sistemi e dati, sottrazione di dati, violazioni del domicilio informatico aziendale, frodi informatiche, danneggiamenti informatici, data breach, reati informatici e abuso delle risorse aziendali di lavoro, ipotesi di reato, relative a:

- Tutela del patrimonio, ivi incluso quello derivante dalla proprietà intellettuale;
- Tutela dei dati aziendali; di quelli professionali; di quelli dei dipendenti e/o dei terzi;
- Tutela della salute e sicurezza dei dipendenti e/o di terzi;
- Commissione di reati e in genere violazione delle regole derivanti dai doveri di protezione incombenti su RCS in ragione dell'adempimento di obbligazioni di Legge, nonchè derivanti dal D.LGS. 231/01;
- In ogni caso di richiesta di Pubbliche autorità, nazionali o internazionali.

Fuor da tali ipotesi, i dati raccolti anche ai fini della prova per la tutela dei diritti della Società o di terzi, non potranno essere utilizzati nell'ambito del rapporto di lavoro a fini disciplinari. I dati non saranno utilizzati ai fini di riconoscimenti professionali.

g) Qualora emerga la necessità di fare un utilizzo nell'ambito del rapporto di lavoro dei dati previsti al punto che precede (escluse eventuali necessità di riservatezza per richieste delle Pubbliche autorità e/o per prevenire e/o impedire il protrarsi o il perpetrarsi di comportamenti criminosi: c.d. controlli occulti), i controlli dei dati raccolti avverranno con le seguenti modalità:

- preavviso di 24 ore, compatibilmente con le attività in corso, da comunicarsi al Data Privacy Officer (DPO) o persona da questi autorizzata al soggetto sindacale identificato al punto b);
- la verifica dei dati raccolti per l'utilizzo nel rapporto di lavoro, che avverrà con la presenza del *Data Privacy Manager* o persona da questi autorizzata e del soggetto sindacale identificato al punto b), è coperta da vincolo di segretezza e riservatezza e avviene con le garanzie della normativa sulla privacy, che vengono assunte in proprio dal rappresentante sindacale;
- In caso di controlli occulti, verrà data informazione al soggetto sindacale di cui al punto b) appena ricevuta l'autorizzazione della Pubblica Autorità e/o terminata la situazione di necessitata riservatezza o urgenza.

Le Parti, considerate anche le modalità di svolgimento dell'incontro odierno, sottoscrivono a distanza il presente accordo. In particolare, I componenti della RSU di Milano presenti nella sede aziendale sottoscrivono in originale contestualmente ai rappresentanti della Società. Copia dell'accordo da questi sottoscritto è inviato a mezzo e-mail ai componenti della RSA di Roma collegati in videoconferenza. I componenti sindacali collegato in videoconferenza appongono la propria sottoscrizione al documento ricevuto e lo inviano tempestivamente all'Azienda (all'indirizzo e-mail vito.ribaudo@rcs.it).

Letto, approvato e sottoscritto.

Milano, 12 aprile 2021

RCS MediaGroup SpA

RSU Quotidiani

RSU MediaGroup

RSA Roma via Campania

Email Protection: Descrizione del servizio

Nome	Finalità	Descrizione	Tipologia di dati trattati	Fornitore
Email Protection	Filtrare la mail aziendale, eliminando quanto più possibile messaggi di Spam, messaggi di Phising, messaggi veicolo di malware. Fornire informazioni dettagliate in merito al tipo di minacce e a chi vengono indirizzate.	Da alcuni anni tutte le analisi svolte in tema di sicurezza mostrano che il veicolo principale attraverso il quale il malware entra in azienda è la mail. Per questo motivo è importante proteggere questo flusso di comunicazione con una tecnologia quanto più aggiornata ed efficace possibile. La posta aziendale viene protetta: • Durante la consegna: Messaggi che contengono spam, malware o link di phishing riconosciuti vengono fermati prima di essere consegnati all'utente. • Dopo la consegna: I link contenuti nelle mail vengono riscritti in modo che un controllo in tempo reale effettuato al momento del "click" dell'utente blocchi la navigazione verso destinazioni riconosciute come pericolose. Eventuali messaggi riconosciuti come pericolosi dopo la consegna nella mailbox dell'utente vengono rimossi automaticamente.	Come per tutti i sistemi di posta vengono acquisiti dati relativi a: • Data/ora di consegna o invio del messaggio • Chi sono i destinatari / mittenti • Oggetto della mail • Esito dei controlli di sicurezza effettuati: messaggio consegnato oppure bloccato e perché. In caso di messaggi contenenti minacce vengono esposti agli operatori autorizzati dati di dettaglio in merito alla tipologia della minaccia stessa: • Esempi di mail veicolanti la minaccia • Famiglia di appartenenza • Diffusione dentro e fuori l'azienda • Chi l'ha ricevuta e chi ha cliccato su un link prima che venisse riconosciuto come pericoloso. • Azioni svolte in caso di esecuzione/click	Proofpoint

Indispensabilità e minimizzazione del trattamento	Gli elementi analizzati, all'interno delle mail e relativi allegati, sono ristretti a quelli che possono contenere minacce, in particolare link. Per proteggersi da eventuali falsi positivi, fenomeno ridotto ma pur sempre possibile, le mail bloccate vengono quarantenate. Operatori autorizzati possono recuperare mail dalla quarantena ed indirizzarle ai destinatari originali o ad altri destinatari (per esempio per effettuare una analisi approfondita della minaccia contenuta) In nessun caso viene acquisito od esposto all'operatore il contenuto delle mail e dei relativi allegati.

End point Detection and Response («EDR») : Descrizione del servizio

Nome	Finalità	Descrizione	Tipologia di dati trattati	Fornitore
End point Detection and Response («EDR»)	Proteggere l'EndPoint da attacchi conosciuti (già indirizzati dagli antivirus tradizionali) e non conosciuti, in tempo reale ed automatizzando anche, ove possibile, le azioni di rimedio (eliminazione della minaccia e ripristino delle azioni malevole compiute) Il servizio verrà realizzato con un prodotto scelto fra due leader di mercato, che operano in maniera analoga: Falcon (Crowdstrike) e Cynet.	L'evoluzione nella tipologia e nel numero di minacce esistenti ha reso obsolete le tecnologie incentrate sull'individuazione di malware già conosciuti. Le tecnologie EDR moderne costituiscono una evoluzione della protezione in quanto aggiungono alla identificazione di malware già noto, il riconoscimento di comportamenti anomali, identificati secondo modelli di attacco continuamente aggiornati. In questo modo diventa possibile riconoscere malware fino a quel momento sconosciuto e/o riconoscere un attacco nelle fasi iniziali del suo svolgimento impedendo che possa andare a buon fine. Se le azioni rilevate identificano un comportamento sicuramente associato ad un malware o identificato come anomalo rispetto al comportamento usuale di un certo Endpoint/Utente, queste vengono bloccate automaticamente e portate all'attenzione dell'operatore tramite la segnalazione di un allarme che contiene tutte le informazioni relative al "quando" e "perché" è stato effettuato il blocco. Tali informazioni non comprendono mai il contenuto di eventuali documenti coinvolti nel blocco.	Per poter svolgere efficacemente le azioni descritte, vengono acquisiti in continuo metadati relativi al funzionamento dell'endpoint. Per "metadati" si intendono i dati relativi alle azioni compiute dai vari software in esecuzione o dai vari utenti. Tra i più significativi: • Processi Eseguiti • File/Cartelle Acceduti • Indirizzi/Siti esterni contattati o dai quali si viene contattati • Altri PC contattati sulla rete aziendale • Frequenza del login e macchine dalle quali viene effettuato	• Cynet • Crowdstrike

Indispensabilità e minimizzazione del trattamento	Non viene acquisito od esposto all'operatore il contenuto dei documenti presenti nel computer, essendo irrilevante nel determinare il profilo di sicurezza di quanto accade su un endpoint. Le informazioni acquisite sono rese disponibili ad operatori appositamente autorizzati o a servizi di Threat Hunting, forniti dal produttore, ciò consente: sia la ricerca e la correlazione di attività anomale che possano essere indice della preparazione di un attacco o della presenza di malware non ancora riconosciuto, sia, in seguito alla segnalazione di un allarme, l'individuazione sulla rete aziendale di Endpoint che possano essere interessati da problematiche simili.

Security Information and Event Management (SIEM): Descrizione del servizio

Nome	Finalità	Descrizione	Tipologia di dati trattati	Fornitore
Security Information & Event Management	Consolidare e correlare tra loro le informazioni provenienti dalle tecnologie di sicurezza adottate dall'azienda, in particolare attraverso i cosiddetti log. Fornire una piattaforma per la gestione degli incidenti.	Un SIEM fornisce un'unica console di gestione dove fare confluire tutte le informazioni provenienti dalle tecnologie di sicurezza, aumentando l'efficacia e l'efficienza degli operatori. Queste informazioni inoltre, vengono correlate tra loro ed analizzate mediante modelli predefiniti che rilevano una concatenazione di eventi anomali o che si discostano da quello che è stato osservato come comportamento usuale di una macchina o di un utente ed ha possibili implicazioni di sicurezza. Tutto questo aumenta l'efficacia delle tecnologie prese singolarmente e consente di rilevare eventi (per esempio di data exfiltration) difficilmente rilevabili altrimenti.	La tecnologia acquisisce ed elabora dati forniti dalle tecnologie di sicurezza e/o di monitoraggio già presenti in azienda. Non aggiunge dati che non siano già presenti ma, mediante una elaborazione intelligente degli stessi è in grado di evidenziare comportamenti di macchine o utenti relazionabili con un rischio di sicurezza (furto di dati, presenza di malware ecc ...) e che come tali devono essere analizzati.	Da definire tra i leader di mercato (es. IBM QRadar, Securonix, Splunk)

Indispensabilità e minimizzazione del trattamento	Non vengono acquisite od esposte all'operatore informazioni aggiuntive rispetto a quelle già raccolte/elaborate dalle tecnologie di sicurezza che il SIEM correla tra loro.