Misure organizzative/procedurali
Verifica della consistenza e disponibilità offline dei backup necessari al rispristino in particolare dei servizi di core business.
Identificazione dei flussi informativi e delle componenti direttamente interconnesse con partner e/o localizzate presso reti ucraine.
Implementazione di una zona demilitarizzata (demilitarized zone – DMZ) per le connettività Business-to-Business (B2B)
Identificazione degli asset critici per lo svolgimento delle principali attività (e.g. processi di business).
Applicazione del principio di privilegio minimo (least privilege) per i sistemi con relazioni di trust e/o con la possibilità di accesso da remoto.
Incremento delle attività di monitoraggio e logging.
Aggiornamento dei piani di gestione degli incidenti cyber in base alle eventuali modifiche architetturali introdotte.
Creazione, aggiornamento, mantenimento ed esercizio periodico di capacità di incident response, di un piano di continuità operativa e resilienza in caso di perdita di accesso o controllo di un ambiente informatico (IT) e/o operativo (OT).
Designazione di un team di risposta alle crisi con i principali punti di contatto, ruoli/responsabilità all'interno dell'organizzazione, inclusi tecnologia, comunicazioni, legal e continuità aziendale.
Assicurare la disponibilità del personale chiave, identificare i mezzi necessari a fornire un supporto immediato per la risposta agli incidenti.
Esercitare il personale nella risposta agli incidenti informatici assicurandosi che tutti i partecipanti comprendano i loro ruoli e compiti specifici.
Prestare particolare attenzione alla protezione degli ambienti cloud prima di trasferire file rilevanti per le attività della propria organizzazione. Inoltre, si raccomanda di utilizzare i controlli di sicurezza resi disponibili dalle piattaforme cloud.
Incrementare le attività di info-sharing con le strutture di sicurezza informatica con particolare riferimento allo CSIRT Italia.
Misure tecniche
Prioritizzazione delle attività di patching dei sistemi internet-facing.
Verifica delle interconnessioni tra la rete IT e le reti OT prediligendo la massima segregazione possibile tra le stesse.
Monitoraggio degli account di servizio e degli account amministrativi per rilevare eventuali attività anomale.
Monitoraggio dei Domain Controller, in particolare gli eventi Kerberos TGS (ticket-granting service), al fine di rilevare eventuali attività anomalie.
Ricerca di processi e/o esecuzione di programmi da linea di comando che potrebbero indicare il dump di credenziali, in particolare monitorando i tentativi di accesso o di copia del file ntds.dit da un Domain Controller.
Monitoraggio dell'installazione di software di trasferimento file quali FileZilla e rclone, nonché dei processi associati agli strumenti di compressione o archiviazione.
Monitoraggio del traffico di rete analizzando picchi anomali nella connettività di rete in uscita, in particolare verso destinazioni inusuali quali provider VPS e VPN, nonché la rete TOR.
Prioritizzare le analisi a seguito di individuazione di codice malevolo (es. Cobalt Strike e webshell).

Assicurarsi che tutti gli accessi remoti richiedano l'autenticazione a più fattori (MFA), in particolare per servizi VPN, portali aziendali rivolti verso l'esterno (extranet) e accesso alla posta elettronica (es. OWA o Exchange Online).