RANSOMWARE

Misure di protezione e organizzazione dei dati per un ripristino efficace

agosto 2021

INDICE

1. Introduzione

In esito agli sviluppi che gli attacchi ransomware hanno avuto negli ultimi tempi ed a seguito della precedente pubblicazione riguardante le misure di protezione (https://csirt.gov.it/contenuti/ransomware-evoluzione-e-misure-di-protezione) nei confronti di questo tipo di minaccia, il presente documento mira all'individuazione di buone pratiche di organizzazione dei dati che facilitino il ripristino a seguito di un attacco.
Per l'individuazione delle misure è stato preso come riferimento il Framework Nazionale per la Cybersecurity e la Data Protection (FNCS), il quale, si ricorda, condivide le misure di sicurezza del Cybersecurity Framework del NIST[1] ed è stato utilizzato quale base di partenza per le misure volte a garantire elevati livelli di sicurezza definite dal DPCM del 14 aprile 2021, n. 81.
Per ridurre la probabilità che un attacco vada a buon fine, diventa essenziale applicare un approccio basato sulla gestione del rischio, integrando all'interno delle procedure aziendali sulla valutazione dei rischi cyber, la minaccia associata al ransomware, recentemente evolutasi con il fenomeno della double extortion, in cui prima di cifrare e rendere irrecuperabili i dati questi vengono esfiltrati, consentendo così agli attaccanti di avere una doppia leva per estorcere denaro alle vittime.
Rivedere regolarmente le misure di sicurezza relative alla protezione e all'organizzazione dei dati critici e integrarle/formalizzarle all'interno dei propri piani di continuità operativa (Business Continuity Plan – BCP), diventa essenziale in ottica di un ripristino efficace dei dati a seguito di attacchi andati a buon fine. Il processo di creazione di quei meccanismi di prevenzione e ripristino, che garantiscano la continuità di servizio a seguito di incidenti, deve partire dallo studio di quanto posto in essere (AS-IS) in termini di misure di sicurezza, fino a definire il target (TO-BE) ed una roadmap per il raggiungimento di tale obiettivo.
Il presente documento definisce un "profilo" del FNCS, ovvero una selezione di subcategory, particolarmente attinenti all'organizzazione dei dati per garantire un efficace ripristino a seguito di attacchi ransomware. Il profilo è corredato da una guida alla lettura e, per ogni pratica di sicurezza, una breve descrizione che ne motiva la selezione. Ad ogni subcategory corrisponde anche una lista di "informative references" tratta dal FNCS alla quale è stato aggiunto, quando presente, il riferimento alle misure del DPCM del 14 aprile 2021, n. 81.
La selezione di subcategory può essere utilizzata per aggiornare, qualora già definita, o delineare la propria roadmap volta ad incrementare la resilienza dell'organizzazione, grazie all'efficace recupero di dati e funzionalità, a seguito di attacchi ransomware.

[1] https://www.nist.gov/cyberframework

2. Riferimenti

Si riportano di seguito alcuni riferimenti che possono supportare la lettura del documento e l'implementazione delle misure suggerite.

- RANSOMWARE: Evoluzione e misure di protezione (CSIRT Italia – Maggio 2021) https://csirt.gov.it/contenuti/ransomware-evoluzione-e-misure-di-protezione la precedente pubblicazione dello CSIRT sul tema ransomware, presenta, oltre all'evoluzione della tipologia dei malware e delle infrastrutture di gestione degli stessi, una descrizione delle diverse fasi dell'attacco, i possibili impatti, un elenco di misure utili a ridurre il rischio e un caso di studio attraverso l'analisi di Egregor;
- Framework Nazionale per la Cybersecurity e la Data Protection (CIS-Sapienza – CINI 2019) https://www.cybersecurityframework.it/ costituisce uno strumento operativo per organizzare i processi di cybersecurity adatto alle organizzazioni pubbliche e private, di qualunque dimensione. È stato preso come riferimento per definire il profilo presentato da questo documento. Associa ad ogni misura di sicurezza (subcategory) una serie di riferimenti utili all'implementazione, tratti dai principali standard sul tema, oltre a dei riferimenti specifici del contesto italiano;
- Misure minime di sicurezza ICT per le pubbliche amministrazioni (AgID 2017) https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict costituiscono un riferimento pratico per valutare e migliorare il livello di sicurezza informatica delle amministrazioni, al fine di contrastare le minacce informatiche più frequenti. Le misure sono già correlate e referenziate nelle informative references del FNCS;
- DPCM del 14 aprile 2021, n. 81 https://www.gazzettaufficiale.it/eli/id/2021/06/11/21G00089/sg regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza. Nell'allegato B definisce, sempre in relazione al FNCS, misure volte a garantire elevati livelli di sicurezza dei beni ICT ai sensi dell'articolo 1, comma 3, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133 (perimetro di sicurezza nazionale cibernetica);
- Cybersecurity Framework Profile for Ransomware Risk Management (NIST) https://csrc.nist.gov/publications/detail/nistir/8374/draft il documento, ancora in versione draft, è pubblicato dal NIST e definisce un profilo sul "core" del Cybersecurity Framework del NIST, specifico per il contrasto alla minaccia di tipo ransomware.

3. Profilo per una corretta organizzazione dei dati e il ripristino efficace

In questa sezione viene riportato il profilo concernente le misure di protezione e organizzazione dei dati per un ripristino efficace a seguito di attacco ransomware. Il profilo è costituito da una selezione di 33 subcategory, per ognuna delle quali sono stati associati una descrizione per l'applicazione, al contesto in esame, della misura di sicurezza e le informative references del FNCS, alle quali è stato aggiunto il DPCM del 14 aprile 2021, n.81.

Guida alla lettura del profilo

Il profilo elenca tutte quelle misure di sicurezza ritenute utili o in qualche modo correlate alla corretta organizzazione e gestione dei dati in previsione di eventuali attacchi ransomware. La singola subcategory, di per sé, non fornisce informazioni di livello tecnico sufficienti a guidarne l'implementazione, pertanto, occorre utilizzare i documenti referenziati nella colonna "informative references" (o le loro versioni più aggiornate) per procedere all'attuazione nell'organizzazione. La colonna "Applicazione al contesto ransomware" fornisce le motivazioni che hanno guidato l'inclusione della subcategory nel profilo ed ulteriori informazioni utili a contestualizzare la misura di sicurezza all'obiettivo preposto.

Function	Category	Subcategory	Applicazione al contesto ransomware	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**ID.AM-1:** Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	Disporre di un inventario esaustivo di tutti gli apparati fisici, comprese le unità di storage, presenti nell'organizzazione consente un più agevole ripristino della funzionalità a seguito di un attacco di tipo ransomware, l'individuazione rapida di tutti i dispositivi che possono contenere dati oggetto dell'eventuale esfiltrazione e/o cifratura ed un ripristino più efficace qualora fosse necessario reinstallare software sui dispositivi.	· **CIS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8, PM-5 · **Misure Minime AgID ABSC 1** · **DPCM 14 aprile 2021, n. 81** 2.1.1
		ID.AM-2: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione	Un censimento dei software in uso, che comprenda almeno vendor, nome e versione nonché il dispositivo su cui è installato (con riferimento all'inventario di cui all'ID.AM-1) ed eventuale lista di patch installate e data degli ultimi aggiornamenti effettuati supporta le attività di analisi e recupero a seguito di eventuale attacco. Con riferimento alla gestione dei dati, l'inventario dei software consente di creare una corrispondenza tra i software e i dati che questi necessitano e trattano.	· **CIS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 · **NIST SP 800-53 Rev. 4** CM-8, PM-5 · **Misure Minime AgID ABSC 2** · **DPCM 14 aprile 2021, n. 81** 2.1.2
		ID.AM-3: I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati	L'identificazione dei flussi dei dati (da quali e verso quali dispositivi e reti transitano) consente l'individuazione delle informazioni e processi a rischio in caso di attacco e di prevedere i possibili percorsi degli attaccanti in caso di movimenti laterali.	· **CIS CSC** 12 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8 · **Misure Minime AgID** ABSC 5.1.4, 13.3.1, 13.4.1, 13.6, 13.7.1, 13.8.1

Function	Category	Subcategory	Applicazione al contesto ransomware	Informative References
		ID.AM-5: Le risorse (es: hardware, dispositivi, dati, allocazione temporale, personale e software) sono prioritizzate in base alla loro classificazione (e.g. confidenzialità, integrità, disponibilità), criticità e valore per il business dell'organizzazione	Classificare i dati in base al livello di criticità che questi rivestono all'interno dell'organizzazione ed attuare misure di protezione a complessità crescente, in accordo a tale classificazione, consente di ottimizzare le risorse a disposizione. Ciò al fine sia di rendere più difficile il lavoro degli attaccanti, sia di individuare chiaramente quali porzioni di dati sono critiche e necessitano, ad esempio, di backup più frequenti e in siti isolati.	· **CIS CSC** 13, 14 · **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.6 · **ISO/IEC 27001:2013** A.8.2.1 · **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6 · **Misure Minime AgID** ABSC 13.1.1, 13.2.1
		DP-ID.AM-7: Sono definiti e resi noti ruoli e responsabilità inerenti al trattamento e la protezione dei dati personali per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	Specie in caso di gestione degli incidenti, risulta particolarmente utile l'individuazione di referenti e responsabili in grado di agevolare le fasi di contenimento e recupero. Ciò non solo in caso di trattamento di dati personali, come previsto per legge, ma anche per il trattamento dei dati critici dell'organizzazione, dei clienti e dei partner.	· **GDPR** - Artt. 24, 26-29, 37-39 · **D.Lgs. 30/6/2003 n. 196** Artt. 2-quaterdecies, 2-quinquiesdecies, 2-sexiesdecies · **ISO/IEC 29100:2011** 4.2, 4.3, 5.10
	Business Environment (ID.BE): La mission dell'organizzazione, gli obiettivi, le attività e gli attori coinvolti sono compresi e valutate in termini di priorità. Tali informazioni	**ID.BE-4:** Sono identificate e rese note interdipendenze e funzioni fondamentali per la fornitura di servizi critici	Dal momento che le funzioni fondamentali spesso dipendono dai dati che trattano, specie in caso di servizi critici, occorre identificare a priori da quali dati dipendono quali funzioni. Questo permette di organizzare le funzioni critiche in modo da scongiurare effetti a cascata in caso di attacco che renda indisponibili anche solo una porzione delle informazioni.	· **COBIT 5** APO10.01, BAI04.02, BAI09.02 · **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 · **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14

Function	Category	Subcategory	Applicazione al contesto ransomware	Informative References
	influenzano i ruoli, le responsabilità di cybersecurity e le decisioni in materia di gestione del rischio.	**ID.BE-5:** Sono identificati e resi noti i requisiti di resilienza a supporto della fornitura di servizi critici per tutti gli stati di esercizio (es. sotto stress/attacco, in fase di recovery, normale esercizio)	I requisiti di resilienza dovrebbero essere definiti anche per i dati che i servizi critici utilizzano, tenendo opportunamente conto dei flussi di cui alla ID.AM-3 e delle interdipendenze di cui alla ID.BE-4.	· **COBIT 5** BAI03.02, DSS04.02 · **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 · **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-13, SA-14
	Governance (ID.GV): Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella gestione del rischio di cybersecurity.	**ID.GV-4:** La governance ed i processi di risk management includono la gestione dei rischi legati alla cybersecurity	Il rischio derivante dai ransomware moderni (cifratura dei dati ed esfiltrazione) deve essere opportunamente considerato nei processi di risk management dell'organizzazione.	· **COBIT 5** EDM03.02, APO12.02, APO12.05, DSS04.02 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 · **ISO/IEC 27001:2013** Clause 6 · **NIST SP 800-53 Rev. 4** SA-2, PM-3, PM-7, PM-9, PM-10, PM-11 · **D.Lgs. 18/5/2018 n. 65 Artt. 12(1), 14(1)** · **DPCM 14 aprile 2021, n. 81** 2.2.2
	Risk Assessment (ID.RA): L'impresa		La comprensione degli impatti potenziali di un attacco ransomware all'interno dell'organizzazione	· **CIS CSC** 4 · **COBIT 5** DSS04.02

Function	Category	Subcategory	Applicazione al contesto ransomware	Informative References
	comprende il rischio di cybersecurity inerente l'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.	**ID.RA-4:** Sono identificati i potenziali impatti sul business e le relative probabilità di accadimento	consente di raffinare l'analisi costi-benefici e prioritizzare le attività volte alla risposta ed al recupero, oltre a supportare le decisioni durante l'eventuale gestione dell'evento cibernetico.	· **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.16.1.6, Clause 6.1.2 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-14, PM-9, PM-11 · **Misure Minime AgID** ABSC 4.8.1
	Supply Chain Risk Management (ID.SC): Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione	**ID.SC-5:** La pianificazione e la verifica della risposta e del ripristino sono condotti con i fornitori e i partner terzi	È utile valutare con eventuali fornitori di storage remoto le politiche di backup e ripristino dei dati e tenerne conto in fase di analisi dei rischi derivanti da ransomware.	· **CIS CSC** 19, 20 · **COBIT 5** DSS04.04 · **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 · **ISA 62443-3-3:2013** SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 · **ISO/IEC 27001:2013** A.17.1.3 · **NIST SP 800-53 Rev. 4** CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9

Function	Category	Subcategory	Applicazione al contesto ransomware	Informative References
	del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.			
	Data Management (DP-ID.DM): i dati personali sono trattati attraverso processi definiti, in coerenza con le normative di riferimento.	**DP-ID.DM-1:** Il ciclo di vita dei dati è definito e documentato	Politiche di distruzione dei dati non più necessari, ed in generale la corretta gestione del ciclo di vita del dato, riducono la superficie di attacco e di conseguenza la possibilità che terzi accedano a porzioni obsolete di dati, le quali potrebbero comunque risultare sensibili (rif. PR-IP.6).	· **GDPR** - Art. 5,6,9-11, 30
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** L'accesso agli asset fisici e logici ed alle relative risorse è limitato al	**PR.AC-4:** I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni	Applicare il principio del privilegio minimo anche all'accesso ai dati risulta di fondamentale importanza per limitare l'impatto di eventuali attacchi.	· **CIS CSC** 3, 5, 12, 14, 15, 16, 18 · **COBIT 5** DSS05.04 · **ISA 62443-2-1:2009** 4.3.3.7.3 · **ISA 62443-3-3:2013** SR 2.1 · **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5

Function	Category	Subcategory	Applicazione al contesto ransomware	Informative References
	personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate			· **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 5.1.1, 5.1.2, 5.1.3, 13.9.1 · **GDPR** - Artt. 25, 32 · **ISO/IEC 29100:2011** 5.11 · **DPCM 14 aprile 2021, n. 81** 3.1.4
	Data Security (PR.DS): I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	**PR.DS-1:** I dati memorizzati sono protetti	Qualora possibile occorre implementare meccanismi per proteggere la confidenzialità delle informazioni memorizzate (data at rest), quali ad esempio, configurazioni e regole appropriate per i firewall e i gateway, l'utilizzo di IDS/IPS, l'utilizzo di crittografia.	· **CIS CSC** 13, 14 · **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 · **ISA 62443-3-3:2013** SR 3.4, SR 4.1 · **ISO/IEC 27001:2013** A.8.2.3 · **NIST SP 800-53 Rev. 4** MP-8, SC-12, SC-28 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 13.3.1 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011 5.11** · **DPCM 14 aprile 2021, n. 81** 3.1.1

Function	Category	Subcategory	Applicazione al contesto ransomware	Informative References
		PR.DS-4: I sistemi hanno adeguate risorse a disposizione per poter garantire la disponibilità	Un elevato grado di ridondanza dei dati, specie quelli individuati quali critici, ottenibile tramite l'utilizzo di tecniche di replicazione (hot-replica e cold-replica) può risultare utile al recupero di dati a seguito di attacco ransomware. In base alla criticità del dato occorre valutare l'opportunità di avere le repliche su siti remoti o comunque su porzioni di rete segmentate.	· **CIS CSC** 1, 2, 13 · **COBIT 5** APO13.01, BAI04.04 · **ISA 62443-3-3:2013** SR 7.1, SR 7.2 · **ISO/IEC 27001:2013** A.12.1.3, A.17.2.1 · **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.DS-5: Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak).	Il fenomeno della double extortion è estremamente comune nei ransomware attuali, di conseguenza le tecniche di data leak prevention giocano un ruolo fondamentale nel contrasto a questo tipo di minaccia.	· **CIS CSC** 13 · **COBIT 5** APO01.06, DSS05.04, DSS05.07, DSS06.02 · **ISA 62443-3-3:2013** SR 5.2 · **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 · **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 13.2.1, 13.7.1, 13.8.1, 13.9.1

Function	Category	Subcategory	Applicazione al contesto ransomware	Informative References
				· **GDPR** - Art. 32 · **ISO/IEC 29100:2011 5.11** · **DPCM 14 aprile 2021, n. 81** 3.3.3
		PR.DS-7: Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione	Isolare (anche logicamente) reti e dati permette di aumentare la sicurezza dell'infrastruttura lasciando gli ambienti soggetti agli stessi controlli operativi. In un'ottica di ripristino efficace permette di aumentare la resilienza anche a seguito di un attacco.	· **CIS CSC** 18, 20 · **COBIT 5** BAI03.08, BAI07.04 · **ISO/IEC 27001:2013** A.12.1.4 · **NIST SP 800-53 Rev. 4** CM-2 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 4.10.1, 8.2.3 · **DPCM 14 aprile 2021, n. 81** 3.3.5
	Information Protection Processes and Procedures (PR.IP): Sono attuate e adeguate nel tempo politiche di sicurezza	**PR.IP-4:** I backup delle informazioni sono eseguiti, amministrati e verificati	Politiche di backup periodici di dati sono eseguite secondo procedure documentate, da personale autorizzato e competente. La verifica dei backup permette di garantire l'integrità del dato. In base alla criticità del dato occorre valutare l'opportunità	· **CIS CSC** 10 · **COBIT 5** APO13.01, DSS01.01, DSS04.07 · **ISA 62443-2-1:2009** 4.3.4.3.9 · **ISA 62443-3-3:2013** SR 7.3, SR 7.4

Function	Category	Subcategory	Applicazione al contesto ransomware	Informative References
	(che indirizzano scopo, ambito, ruoli e responsabilità, impegno da parte del management e coordinamento tra le diverse entità organizzative), processi e procedure per gestire la protezione dei sistemi informativi e degli assets.		di avere le repliche su siti remoti o comunque su porzioni di rete segmentate.	· **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 · **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 10.1, 10.2.1, 10.4.1 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11 · **DPCM 14 aprile 2021, n. 81** 3.4.3
		PR.IP-6: I dati sono distrutti in conformità con le policy	Politiche di distruzione dei dati non più necessari, ed in generale la corretta gestione del ciclo di vita del dato, riducono la superficie di attacco e di conseguenza la possibilità che terzi accedano a porzioni obsolete di dati, le quali potrebbero comunque risultare sensibili.	· **COBIT 5** BAI09.03, DSS05.06 · **ISA 62443-2-1:2009** 4.3.4.4.4 · **ISA 62443-3-3:2013** SR 4.2 · **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 · **NIST SP 800-53 Rev. 4** MP-6 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **GDPR** - Art. 5, 17, 32 · **ISO/IEC 29100:2011** 5.11
	Maintenance (PR.MA): La manutenzione dei sistemi informativi e di controllo	**PR.MA-1:** La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati	Garantire l'affidabilità del servizio di manutenzione e riparazione permette di ridurre la superficie d'attacco anche rispetto al cosiddetto "fattore umano". L'integrità dei sistemi e dei dati viene preservata.	· **COBIT 5** BAI03.10, BAI09.02, BAI09.03, DSS01.05 · **ISA 62443-2-1:2009** 4.3.3.3.7 · **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6

Function	Category	Subcategory	Applicazione al contesto ransomware	Informative References
	industriale è fatta in accordo con le politiche e le procedure esistenti.			· **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5, MA-6 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 4.5, 8.2.2
		PR.MA-2: La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati	Politiche di accesso da remoto alle risorse permettono, tramite personale qualificato, di mantenere sistemi e dati coerenti con gli obiettivi con la continuità del processo.	· **CIS CSC** 3, 5 · **COBIT 5** DSS05.04 · **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 · **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 · **NIST SP 800-53 Rev. 4** MA-4 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 3.4.1, 8.2.2
	Protective Technology (PR.PT): Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le	**PR.PT-3:** Viene adottato il principio di minima funzionalità configurando i sistemi in modo che forniscano solo le funzionalità necessarie	Qualora applicata correttamente, solo utenti privilegiati accedono a porzioni di dati più sensibili. Risulterebbe inoltre più complesso per l'attaccante accedere a grandi porzioni di dati: ogni utente dovrebbe poter accedere solo ai dati di cui ha effettivamente bisogno.	· **CIS CSC** 3, 11, 14 · **COBIT 5** DSS05.02, DSS05.05, DSS06.06 · **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4

Function	Category	Subcategory	Applicazione al contesto ransomware	Informative References
	relative politiche, procedure ed accordi.			· **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 · **ISO/IEC 27001:2013** A.9.1.2 · **NIST SP 800-53 Rev. 4** AC-3, CM-7 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **Misure Minime AgID** ABSC 5.1.1, 5.1.2, 5.1.3, 5.9.1, 8.3.1 · **GDPR** - Art. 32 · **ISO/IEC 29100:2011** 5.11
		PR.PT-5: Sono implementati meccanismi (es. failsafe, load balancing, hot swap) che permettono di soddisfare requisiti di resilienza sia durante il normale esercizio che in situazioni avverse	Valutare l'implementazione di controlli fisici e logici compatibili con le funzioni critiche associate al business dell'organizzazione.	· **COBIT 5** BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 · **ISA 62443-2-1:2009** 4.3.2.5.2 · **ISA 62443-3-3:2013** SR 7.1, SR 7.2 · **ISO/IEC 27001:2013** A.17.1.2, A.17.2.1 · **NIST SP 800-53 Rev. 4** CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(1)-(3), 14(1)-(3), 14(13) · **GDPR** - Art. 32 · **ISO/IEC 29100:2011 5.11**

Function	Category	Subcategory	Applicazione al contesto ransomware	Informative References
				· **DPCM 14 aprile 2021, n. 81** 3.6.3
DETECT (DE)	**Anomalies and Events (DE.AE):** Le attività anomale sono rilevate e il loro impatto potenziale viene analizzato.	**DE.AE-2:** Gli eventi rilevati vengono analizzati per comprendere gli obiettivi e le metodologie dell'attacco	La comprensione del reale obiettivo di un attacco subito potrebbe agevolare l'individuazione di eventuali tecniche di persistenza adottate dagli attaccanti e scongiurare quindi la possibilità di reinfezione a beneficio di un ripristino più efficace	· **CIS CSC** 3, 6, 13, 15 · **COBIT 5** DSS05.07 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 · **ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple	Le politiche di correlazione degli eventi e delle informazioni di sicurezza, consentono l'identificazione di un attacco già durante le prime fasi in cui esso si può sviluppare, permettendo di intraprendere nella maniera più veloce le opportune contromisure associate alla salvaguardia e all'integrità dei dati.	· **CIS CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 · **COBIT 5** BAI08.02 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.12.4.1, A.16.1.7 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4 · **Misure Minime AgID ABSC 8.1.3** · **DPCM 14 aprile 2021, n. 81** 4.1.1
		DE.AE-4: Viene determinato l'impatto di un evento	Le organizzazioni possono prepararsi alla risposta efficiente in caso di eventi cyber avversi che interrompono le loro operazioni, sviluppando opportune analisi d'impatto sulle attività di	· **CIS CSC** 4, 6 · **COBIT 5** APO12.06, DSS03.01 · **ISO/IEC 27001:2013** A.16.1.4

Function	Category	Subcategory	Applicazione al contesto ransomware	Informative References
			business (Business Impact Analysis - BIA) e conducendo una valutazione del rischio (Risk Assessment - RA). Prima di creare un piano di continuità operativa (Business Continuity Plan - BCP), un'organizzazione dovrebbe condurre una valutazione dei rischi dettagliata così da identificare le aree di esposizione e tutte le possibili minacce che potrebbero causare un'interruzione dell'attività.	· **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI-4
	Security Continuous Monitoring (DE.CM): I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	**DE.CM-4:** Il codice malevolo viene rilevato	L'identificazione del codice malevolo associato alla minaccia permette di intraprendere nella maniera più veloce le opportune contromisure associate alla salvaguardia e all'integrità dei dati.	· **CIS CSC** 4, 7, 8, 12 · **COBIT 5** DSS05.01 · **ISA 62443-2-1:2009** 4.3.4.3.8 · **ISA 62443-3-3:2013** SR 3.2 · **ISO/IEC 27001:2013** A.12.2.1 · **NIST SP 800-53 Rev. 4** SI-3, SI-8 · **Misure Minime AgID** ABSC 8.1.1, 8.2.2, 8.2.3, 8.5, 8.6.1, 8.7.2, 8.7.3, 8.7.4, 8.8.1, 8.9, 8.10.1, 8.11.1 · **DPCM 14 aprile 2021, n. 81** 4.2.2
RESPOND (RS)	**Response Planning (RS.RP):** Procedure e processi di risposta sono eseguiti e mantenuti per assicurare una risposta agli incidenti	**RS.RP-1:** Esiste un piano di risposta (response plan) e questo viene eseguito durante o dopo un incidente	Le politiche di incident response permettono di identificare e salvaguardare i dati critici, agendo velocemente in caso di necessario ripristino.	· **CIS CSC** 19 · **COBIT 5** APO12.06, BAI01.10 · **ISA 62443-2-1:2009** 4.3.4.5.1 · **ISO/IEC 27001:2013** A.16.1.5 · **GDPR Art. 33** · **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8

Function	Category	Subcategory	Applicazione al contesto ransomware	Informative References
	di cybersecurity rilevati.			· **DPCM 14 aprile 2021, n. 81** 5.1.1
	Mitigation (RS.MI): Vengono eseguite azioni per prevenire l'espansione di un evento di sicurezza, per mitigare i sui effetti e per risolvere l'incidente.	**RS.MI-1:** In caso di incidente vengono messe in atto procedure atte a contenerne l'impatto	Prevenire la diffusione dell'infezione isolando tutti i computer compromessi (gli uni dagli altri, dallo storage condiviso e dalle reti).	· **CIS CSC** 19 · **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.4.5.6 · **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 · **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 · **NIST SP 800-53 Rev. 4** IR-4 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(2), 14(2)-(3) · **Misure Minime AgID** ABSC 8.1.3, 8.4
		RS.MI-2: In caso di incidente vengono messe in atto procedure atte a mitigarne gli effetti	Integrare le procedure di risk assessment della propria organizzazione considerando la minaccia cyber associata ai ransomware garantisce, a valle dello sviluppo di opportuni Business Continuity Plan (BCP), la continuità operativa prima e durante l'esecuzione del ripristino dei dati.	· **CIS CSC** 4, 19 · **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 · **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 · **NIST SP 800-53 Rev. 4** IR-4 · **D.Lgs. 18/5/2018 n. 65** Artt. 12(2), 14(2)-(3) · **Misure Minime AgID ABSC 8.4** · **DPCM 14 aprile 2021, n. 81** 5.4.1
	Improvements (RS.IM): Le attività	**RS.IM-1:** I piani di risposta agli incidenti tengono in	Monitorare e documentare i processi di gestione degli incidenti, aiuta l'organizzazione	· **COBIT 5** BAI01.13 · **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4

Function	Category	Subcategory	Applicazione al contesto ransomware	Informative References
	di risposta sono migliorate incorporando le "lesson learned" da attività precedenti di monitoraggio e risposta.	considerazione le esperienze passate (lesson learned)	nell'implementazione efficiente delle politiche di risposta e recupero.	· **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RECOVER (RC)	**Recovery Planning (RC.RP):** I processi e le procedure di ripristino sono eseguite e mantenute per assicurare un recupero dei sistemi o asset coinvolti da un incidente di cybersecurity.	**RC.RP-1:** Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity	Le politiche di Business Continuity Planning (BCP) dovrebbero includere valutazioni circa il tempo di inattività massimo tollerabile, l'obiettivo del punto di ripristino e il tempo di ritorno alla normale attività. Il tempo necessario per reinserire le informazioni perse e tornare alla piena funzionalità dovrebbe essere minimizzato.	· **CIS CSC** 10 · **COBIT 5** APO12.06, DSS02.05, DSS03.04 · **ISO/IEC 27001:2013** A.16.1.5 · **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8 · **Misure Minime AgID** ABSC 3.2.2
	Improvements (RC.IM): I piani di ripristino ed i relativi processi sono migliorati tenendo conto delle "lesson learned" per le attività future.	**RC.IM-1:** I piani di ripristino tengono in considerazione le esperienze passate (lesson learned)	Monitorare e documentare i processi, aiuta l'organizzazione nell'implementazione efficiente delle politiche di esecuzione dei piani di ripristino di funzionalità e dati critici.	· **COBIT 5** APO12.06, BAI05.07, DSS04.08 · **ISA 62443-2-1:2009** 4.4.3.4 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8 · **Misure Minime AgID** ABSC 3.1.3
		RC.IM-2: Le strategie di recupero sono aggiornate	Rivedere regolarmente le misure di sicurezza relative alla protezione e all'organizzazione dei dati critici e integrarle/formalizzarle all'interno dei	· **COBIT 5** APO12.06, BAI07.08 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10

Function	Category	Subcategory	Applicazione al contesto ransomware	Informative References
			propri piani di continuità operativa (Business Continuity Plan – BCP), diventa essenziale in ottica di un ripristino efficace dei dati a seguito di attacchi andati a buon fine.	· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8

4. Conclusioni

Il presente documento riporta una serie di misure di sicurezza ritenute utili per agevolare il recupero dei dati a seguito di un attacco ransomware. Tali misure sono da considerare quali base necessaria, ma non sufficiente, a garantire una efficace resilienza a seguito di incidente e sono volte principalmente alla gestione dei dati. Il panorama più ampio delle misure di protezione nei confronti di minacce specifiche esula dallo scopo di questo documento, la cui applicazione non può prescindere dall'adozione di un approccio strutturato al problema della sicurezza cibernetica.

Il profilo presentato prende anche spunto da lavori recenti sul tema del NIST ed è stato corredato da una guida alla lettura e da una serie di riferimenti, tra i quali, il recente DPCM del 14 aprile 2021, n. 81, che delinea le misure di sicurezza per i soggetti appartenenti al perimetro di sicurezza nazionale cibernetica.