S.C. I.C.T. & Sistemi Informativi

Relazione sulle misure in tema di cybersecurity

Relazione di riepilogo Anno 2021

Indice generale

1. Premessa

A causa della qualità e della quantità di dati sensibili che vi transitano e che ovviamente generano un grande valore economico, il settore sanitario costituisce uno dei principali bersagli dei cyber criminali. Secondo l'ultimo report di Trend Micro Research, la divisione di Trend Micro leader globale di cybersecurity, la sanità italiana è sempre più nel mirino degli hacker, tanto che nel 2020 è stato il primo settore per numero di attacchi informatici subiti.
Il trend crescente di attacchi è stato confermato anche nel 2021 dove la crescita rispetto all'anno precedente è stata del 24%, mentre quello degli attacchi gravi con finalità di estorsione di denaro sono aumentati del 21%. (fonte rapporto Clusit 2021).
In generale l'Italia si conferma tra le nazioni più attaccate dai cybercriminali risultando terza al mondo per numero di ransomware e quarta per numero di malware (dati di Ottobre 2021).
Le prime iniziative di risposta al problema a livello Nazionale sono state l'istituzione della nuova Agenzia per la Cybersicurezza nazionale e il decreto attuativo del perimetro di sicurezza nazionale cibernetica che pongono la cybersecurity a fondamento della digitalizzazione della Pubblica Amministrazione.
Anche a ciascuna amministrazione locale è richiesto di rafforzare le misure di prevenzione e mitigazione degli attacchi, oltre a predisporre le opportune procedure per la gestione di un eventuale incidente. Le responsabilità in capo a ciascuna amministrazione sono anche richiamati dagli obiettivi previsti dal piano triennale 2021-2022 (e ripresi nell'aggiornamento 2022-2023), ed in particolare:

- OB.6.1 - Aumentare la consapevolezza del rischio cyber (Cyber Security Awareness) nelle PA
  - Entro dicembre 2021 - Le PA valutano l'utilizzo del tool di Cyber Risk Assessment per l'analisi del rischio e la redazione del Piano dei trattamenti - CAP6.PA.LA04
  - Entro marzo 2022 - Le PA definiscono, sulla base di quanto proposto dal RTD, all'interno dei piani di formazione del personale, interventi sulle tematiche di Cyber Security Awareness - CAP6.PA.LA05
  - Entro giugno 2022 - Le PA si adeguano alle Misure minime di sicurezza ICT per le pubbliche amministrazioni aggiornate - CAP6.PA.LA06.
- OB.6.2 - Aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione
  - Da gennaio 2021 - Le PA devono consultare la piattaforma Infosec aggiornata per rilevare le vulnerabilità (CVE) dei propri asset – CAP6.PA.LA07
  - Da maggio 2021 - Le PA devono mantenere costantemente aggiornati i propri portali istituzionali e applicare le correzioni alle vulnerabilità - CAP6.PA.LA08

2. Normativa di Riferimento

La sicurezza cibernetica costituisce uno degli interventi previsti dal Piano nazionale di ripresa e resilenza (PNRR) trasmesso dal Governo alla Commissione europea il 30 aprile 2021.
A livello di Unione europea la direttiva (UE) 2016/1148 del 6 luglio 2016 reca misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (c.d. direttiva NIS - Network and Information Security") al fine di conseguire un "livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea".
La direttiva è stata recepita nell'ordinamento italiano con il decreto legislativo n. 65 del 18 maggio 2018, che detta quindi la cornice legislativa delle misure da adottare per la sicurezza delle reti e dei

sistemi informativi ed individua i soggetti competenti per dare attuazione agli obblighi previsti dalla direttiva NIS.

Successivamente, il decreto-legge n. 105 del 2019 è stato adottato al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati, attraverso l'istituzione di un perimetro di sicurezza nazionale cibernetica e la previsione di misure volte a garantire i necessari standard di sicurezza rivolti a minimizzare i rischi. Talune modifiche sono state apportate, a tale provvedimento, dal decreto-legge n. 162 del 2019, in materia di proroga dei termini e altre disposizioni sulla pubblica amministrazione.
In attuazione del decreto-legge n. 105 sono stati definiti in particolare il DPCM 30 luglio 2020, n. 131, che ha dettato criteri e modalità per l'individuazione dei soggetti inclusi nel perimetro nazionale di sicurezza cibernetica, e il DPCM 14 aprile 2021, n. 81 che definisce le modalità per la notifica nel caso di incidenti riguardanti beni ITC.
Infine, con il decreto-legge 14 giugno 2021, n. 82, si è proceduto alla definizione dell'architettura nazionale di cybersicurezza e all'istituzione dell'Agenzia per la cybersicurezza nazionale.
Si citano inoltre:

- Piano triennale per l'informatica nella Pubblica amministrazione emanato dall'Agenzia per l'Italia Digitale che indica il "*Modello strategico di evoluzione del sistema informativo della Pubblica amministrazione"*, ovvero la visione a medio/lungo termine verso la quale la Pubblica amministrazione deve tendere per sfruttare al meglio i benefici derivanti da un uso corretto, mirato e consapevole delle tecnologie digitali e successivi aggiornamenti.
- Circolare 18 aprile 2017, n.2/2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)», che indica alle pubbliche amministrazioni le misure minime per la sicurezza ICT che debbono essere adottate al fine di contrastare le minacce più comuni e frequenti cui sono soggetti i loro sistemi informativi.
- «Linee guida per la configurazione per adeguare la sicurezza del software di base», che fornisce un insieme di indicazioni per affrontare e risolvere correttamente le problematiche legate alla sicurezza del software di base e di individuare le misure da adottare per difendere ogni componente da possibili minacce accidentali e/o intenzionali.
- «Linee guida per lo sviluppo del software sicuro», relativo alle indicazioni per lo sviluppo del software sicuro nella pubblica amministrazione.
- «Raccomandazioni Agid in merito allo standard Transport Layer Security (TLS)» e determinazione n. 471 del 5 novembre 2020 - Adozione delle Raccomandazioni AgID in merito allo standard Transport Layer Security (TLS).
- Regolamento Europeo 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.
- Decreto legislativo 196/2003 e s.m.i. – Codice per la Protezione dei Dati Personali, aggiornato al D. Lgs. n. 101/2018 in vigore dal 19/9/2018.
- Codice dell'Amministrazione Digitale e successivi decreti che hanno progressivamente integrato e modificato l'originario D. Lgs. n.82/2005.
- D.G.R 27-6517 del 23.02.2018 "Attuazione del Piano Triennale per l'informatica nella P.A. 2017-2019 e degli adempimenti in materia di Sanità digitale. Linee di indirizzo della sanità digitale Piemontese – Progetti regionali 2018-2020";

La norma **ISO 27001** è una norma internazionale che definisce i requisiti per impostare e gestire un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) ed include aspetti relativi alla sicurezza logica, fisica ed organizzativa di un'Azienda.

La norma **UNI EN ISO/IEC 27001:2017** è l'adozione nazionale della norma internazionale ISO/IEC 27001 (edizione ottobre 2013) e tiene conto del corrigendum di settembre 2014 (Cor.1:2014). La norma specifica i requisiti per stabilire, attuare, mantenere e migliorare in modo continuo un sistema di gestione per la sicurezza delle informazioni nel contesto di un'organizzazione. La presente norma internazionale include anche i requisiti per la valutazione e per il trattamento dei rischi relativi alla sicurezza delle informazioni adattati alle necessità dell'organizzazione. I requisiti stabiliti dalla presente norma internazionale sono di carattere generale e predisposti per essere applicabili a tutte le organizzazioni, indipendentemente dalla loro tipologia, dimensione e natura.

La norma **ISO/IEC 27002** consiste sostanzialmente in una raccolta di **"**best practices" che possono essere adottate per soddisfare i requisiti della norma ISO 27001:2005 al fine di proteggere le risorse informative. Ogni sezione della norma è dedicata, infatti, a specifiche aree inerenti alla sicurezza delle informazioni all'interno dell'azienda, a livello di infrastrutture sia tecniche che organizzative

Lo standard **ISO 27701**, di recentissima pubblicazione (agosto 2019) rappresenta lo sviluppo e l'implementazione degli standard precedentemente introdotti dalle ISO 27001 e 27002 di cui si è precedentemente discusso. Lo scopo che la norma si prefissa, sulla base delle novità legislative introdotte dal GDPR, è quello di migliorare gli attuali sistemi di gestione, aggiungendo alle ISO esistenti ulteriori requisiti specifici in ambito di gestione delle informazioni sulla privacy. Per tali motivi, non può prescindere da una lettura congiunta delle ISO cui la stessa si lega, istituendo una serie di controlli specifici per le figure del titolare e del responsabile del trattamento introdotti dal GDPR, dei quali precedentemente non si teneva (almeno espressamente) conto.

3. Misure di sicurezza implementate

Per garantire il massimo livello di protezione e resilienza, l'azienda ha adottato misure di sicurezza diversificate, implementando sistemi di sicurezza informatica stratificati, in modo da rispondere a più livelli alle minacce cyber.
Molte delle misure adottate rientrano nel "Sistema di Gestione per la Sicurezza delle Informazioni" aziendale (SGSI) che, attraverso un approccio continuo ed iterativo basato sul modello Plan-Do-Check-Act, si focalizza sull'individuazione, valutazione, trattamento e documentazione dei rischi associati alla gestione dei sistemi e delle infrastrutture informatiche.
Una descrizione dettagliata delle infrastrutture informatiche e degli strumenti di protezione adottati sono presenti nei documenti:

- Infrastruttura_rete_3 (aggiornato al 18 marzo 2021)
- Misure di sicurezza rev 2 (aggiornato al al 16 marzo 2021)

A fianco del SGSI, per fornire risposte adeguate alla minaccia cyber, si è ritenuto opportuno selezionare un modello per l'incident response che potesse guidare il processo di risposta alle minacce cibernetiche e agli insider threat.

A tal fine è stato selezionato l'Incident response cycle che, attraverso le fasi di preparazione, identificazione, contenimento, eradicazione, ripristino e lesson learned, si ritiene possa aiutare nelle aree di prevenzione, rilevamento e risposta e per lo sviluppo delle strategie di difesa dagli attacchi.
Molta importanza è stato data proprio allo step di preparazione ed in particolare alla fase di harderning con l'obiettivo di ridurre la superficie di attacco.
Parallelamente, per valutare la completezza degli strumenti messi in campo e identificare eventuali gap da colmare, è stata avviata un'analisi che partendo dalle tecniche del framework "Mitre ATT&CK" (Adversarial Tactics, Techniques & Common Knowledge) ha valutato eventuali strumenti di contrasto e risposta per ciascuna tecnica.
Tale attività ha portato ad identificare le seguenti necessità (in ordine di priorità):

- rafforzamento della cybersecurity awareness degli utenti;
- revisione della configurazione dei servizi avanzati della suite Watchguard Total Security presente sui firewall aziendali con eventuale attivazione anche dei moduli Threat Detection & Response e DNS watch;
- completamento dell'attività di patch management e di aggiornamento dei sistemi;
- rafforzamento del protezione delle email attraverso un Security Email Gatawey
- verifica delle ACL degli utenti sulle aree di rete e di dominio ed eventuale introduzione di un sistema PAM (Priviledge AccessManagement) che permetta il monitoraggio e la protezione degli account privilegiati
- eventuale opportunità di affiancare l'attuale strumento di EDR (Endpoint Detection and Reponse) con un SIEM (Security Information and Event Management) e un SOAR (Security Orchestration Automation and Response);
- opportunità di introdurre honeypot;

Nel paragrafo 5.5 "Analisi criticità e individuazione ulteriori misure" è riportata una descrizione più ampia di ciascuna iniziativa valutata.

Si ritiene opportuno elencare brevemente gli strumenti attualmente in funzione in tema di cybersecurity:

- Protezione degli Endpoint (antivirus, antimalware, protezione da ransoware, web filtering, Botnet blocker) => attraverso la piattaforma F-secure Business Suite Premium
- Endpoint Detection and Response => attraverso la piattaforma F-Secure Elements Endpoint Detection and Response
- Firewall perimetrale => Watchguard Firebox M670
- Application control, Intrusion Prevenction Service (IPS), ATP Blocker, Gateway AntiVirus, WebBlocker (filtro contenuti/url) => attraverso la suite Watchguard Total Security all'interno dei firewall aziendali
- Telemetria attraverso diversi strumenti di monitoring: Cisco Prime per il monitoraggio degli switch e della rete, Check MK per i servizi e gli host, telemetria integrata in VmWare vSphere per le VM: sebbene non siano strumenti di cybersecutirty, aiutano il personale tecnico di rilevare anomalie che potrebbero segnalare un attacco in corso o la presenza di malware.
- Attività trimestrali di vulnerability assessment
- Attività di hardening programmata

In generale la strategia di cyber-sicurezza adottata dall'azienda si basa su alcuni aspetti di rilevo. Tra questi:

- Consapevolezza: la comprensione del rischio effettivo e potenziale è la leva per definire priorità di investimento nella protezione del patrimonio informativo aziendale.
- Pianificazione: una corretta pianificazione deve agire con un approccio di lungo termine e, al contempo, eseguire interventi immediati sugli aspetti più critici. Tutto questo è possibile soltanto quando si è definito un piano strategico, affrontando il problema non solo con la "tattica" giusta, ma con la giusta visione di insieme.
- Visione olistica: la continua evoluzione delle tecniche di attacco fa sì che la sicurezza informatica non debba essere vista come un prodotto, ma come un processo. Per questo occorre avere un approccio basato su una visione olistica, per definire i processi, agire in modo sostenibile, definendo priorità e allocazione degli investimenti.
- Security by design: l'adozione di modelli di security by design è determinante per garantire che il software sviluppato e i sistemi installati siano sicuri, sin dalla progettazione e fino alla fase di messa in produzione.
- Interdisciplinarità. Tutte le figure professionali debbono essere coinvolte nei processi di sicurezza considerando che questa non è solo appannaggio delle figure tecniche. Alcune azioni da introdurre per aumentare la resilienza ai rischi cyber richiedono infatti interdisciplinarità, perché il cybercrime stesso agisce con attacchi che si basano sull'amalgama di molte discipline.
- Elemento umano: l'elemento umano è centrale nell'approccio alla cybersecurity, perché occorre agire su diversi soggetti: su chi può subire un attacco cyber (i dipendenti), chi deve difendere la PA da un attacco (gli addetti alla sicurezza aziendale) e chi deve decidere (direzione e governance) in merito a quali investimenti introdurre per ridurre il rischio cyber e come agire tempestivamente a fronte di attacchi subiti.
- Comunicazione. Uno degli elementi critici nelle organizzazioni complesse è la comunicazione con gli stakeholder interni o esterni. È necessario ottimizzare la comunicazione tra il personale tecnico dei Sistemi Informativi (sviluppatori, sistemisti, dba, tecnici manutentori), il personale tecnico dell'Ingegneria Clinica, il personale amministrativo e sanitario e i gruppi dirigenziali. Una condivisione degli obiettivi in tema di sicurezza cibernetica e delle strategie aiuta nel .
- Aggiornamento delle competenze. Non tutte le professioni evolvono così rapidamente come la sicurezza informatica. In un'ottica di sostenibilità della cybersecurity è importante tenere allineate ed aggiornate le competenze delle figure professionali coinvolte nella cybersecurity.

4. Organizzazione personale per attività di sicurezza

Le funzioni di SOC (Security Operation Center) e di CSIRT (Computer Secutiry Incident Response Team) non sono demandate a figure professionali dedicate, ma sono in capo all'intero team dei Sistemi Informativi.
Responsabile della cybersecurity è il dr. Geninatti che in accordo con la direzione dei sistemi informativi individua e propone le misure di sicurezza più opportune da adottare.
L'implementazione delle stesse avviene con l'ausilio del sistemista di presidio, con il personale di rete e con il supporto di specialisti esterni attivati in base alla specifiche necessità.

I controlli sono effettuati oltre che dal personale già citato anche a cura di alcuni tecnici della manutenzione opportunamente istruiti e che svolgono controlli programmati secondo checklist giornaliere, mensili e annuali.
Sono in corso approfondimenti per valutare la possibilità di ingaggiare in tempo reale servizi di CSIRT/CERT on demand.

5. Azioni di rilievo attuate nel 2021

Come descritto in premessa, l'incremento degli attacchi alle infrastrutture pubbliche ed in particolare al settore sanitario ha spinto l'A.O. Mauriziano a rafforzare le misure di sicurezza.
Tra le azioni di rilievo intraprese nel 2021 in quest'ambito si citano:

- l'invio di materiale informativo in tema di sicurezza informatica;
- la predisposizione di un questionario per valutare la consapevolezza del rischio cyber (Cyber Security Awareness) del personale dell'azienda;
- attività di hardering dei sistemi e dell'infrastruttura;
- rafforzamento dei controlli di sicurezza.
- analisi criticità e individuazione delle ulteriori misure necessarie per garantire un adeguato livello di sicurezza cibernetica;

5.1 Invio di materiale informativo sulla sicurezza informatica

Attraverso l'invio di email destinate a tutto il personale dell'azienda, sono stati diffusi alert di sicurezza circa le minacce più attuali e le vulnerabilità maggiormente sfruttate. Ciascuna email descrive sempre i principali elementi di attenzione, richiama i corretti comportamenti da adottare e approfondisce con un linguaggio semplice gli argomenti di sicurezza correlati alla minaccia.

5.2 Questionario di cybersecurity

Al fine di misurare la preparazione e la consapevolezza degli utenti in tema di cybersicurezza è stato predisposto il questionario "Valutazione Conoscenze CyberSecurity" che è stato sottoposto a tutti gli utenti.
La compilazione dello stesso non era obbligatoria e ha visto la partecipazione di 237 utenti contro i circa 1600 utenti coinvolti.
L'elenco delle domande e i dati aggregati delle risposte fornite sono riportate in apposito documento allegato alla presente relazione.
Alcuni degli aspetti emersi dal questionario potrebbero fornire spunti per azioni di miglioramento. Tra questi:

- solo il 34% degli utenti è conoscenza dell'esistenza del regolamento aziendale per l'utilizzo delle risorse informatiche e meno del 29% lo ha consultato. Potrebbe quindi essere opportuno promuovere il documento, magari dopo gli opportuni aggiornamenti.
- Il 34% degli utenti collega (raramente o qualche volta) dispositivi personali (es. chiavetta USB) ai computer aziendali. Il tema andrebbe approfondito e normato. approfondito
- L'11% degli utenti ha provveduto ad installare in autonomia, sui dispositivi aziendali, software o applicazioni non fornite dall'azienda. Questa affermazione trova riscontro anche

con le evidenze rinvenute dal modulo di Application control del sistema di endpoint protection che talvolta rileva software non autorizzato installato (es. TOR browser)

- Si rilevano alcuno comportamenti poco sicuri di una parte degli utenti con percentuali tra il 20% e il 50%. Fra questi:
  - utilizzo della stessa password su differenti account
  - annotazione delle password su supporti cartacei
  - condivisione delle proprie password con i colleghi
  - mancata verifica della sicurezza di un sito prima di inserire informazioni private
  - utilizzo di chiavette USB di cui non si conosce la storia
  - lasciare il PC incustodito con l'utenza sbloccata

  Tali aspetti dovranno essere oggetto di opportuna campagna informativa.
- Una delle domande mostrava due email di cui una potenzialmente rischiosa (tentativo di phishing). Il 66% dei soggetti l'ha riconosciuta come tale, il 14% le ha classificate entrambe come rischiose, mentre il restante 20% non sapeva rispondere o ha indicato la mail sbagliata come malevola. Proprio su quest'ultima categoria di utenti potrebbe costituire un rischio importante e sarà opportuno proseguire l'attività di formazione e rafforzare gli strumenti di email filtering.
- Potrebbe essere opportuno sensibilizzare il personale in merito al tema della sicurezza dei dispositivi medici. Infatti oltre il 70% del campione non ha saputo rispondere correttamente alla domanda che chiedeva di specificare quali dispositivi medici impiantabili tra quelli di un breve elenco, fossero potenzialmente a rischio di attacchi informatici.
- Si rileva infine che il 50% circa del campione ha manifestato interess3 p3r un'eventuale formazione in presenza in tema di sicurezza informatica

5.3 Attività di hardering dei sistemi e dell'infrastruttura

L'attività di hardening è quel processo che mira a ridurre la superficie delle vulnerabilità che posso essere sfruttate per un attacco.
Il processo è continuo perché i sistemi e l'ambiente in cui sono inseriti sono in continua mutazione: l'aggiunta di nuovi servizi, l'installazione o aggiornamento di software, la scoperta di nuove vulnerabilità sui sistemi esistenti, l'integrazione con nuovi sistemi, ma anche l'inserimento di nuovo personale o la cessazione di personale attivo, sono esempi di eventi che richiedono una continua verifica delle corrette configurazioni dei software e dei sistemi.
L'attività svolta nell'anno in esame ha riguardato alcuni punti specifici:

- Verifica regole firewall con chiusura delle porte TCP e UDP non necessarie. L'attività non è terminata e proseguirà nel 2022.
- Disabilitazione utenti zombie: si tratta della disattivazione degli utenti che hanno cessato il loro rapporto di lavoro o di collaborazione con l'azienda (es. dipendenti in pensione, fornitori di servizi il cui ,andato è scaduto, utenze utilizzare su servizi windows dismessi). E' stata fatta una prima verifica delle utenze e il controllo è stato formalizzato affinché venga eseguito mensilmente (controllo SSI004M.5).
- Verifica privilegi utenze: l'attività riguarda la verifica delle autorizzazioni assegnate a ciascun account del sistema, in modo che siano concessi i soli diritti strettamente necessario per i funzionamento di un servizio (per gli utenti di sistema) o per lo svolgimento delle proprie mansioni (per gli utenti personali). Questa attività è applicabile a livello di dominio

e di qualsiasi sistema software. L'attività svolta nel 2021 ha riguardato le utenze di dominio e del sistema di posta elettronica e vede ancora da completare la riduzione dei privilegi di alcuni utenti di dominio con ruoli amministrativi per cui non è stato possibile valutare l'impatto della modifica. Tali utenze saranno esaminate e validate nel 2022.

- Aggiornamento software e installazione patch di sicurezza: l'attività di aggiornamento "ordinaria" eseguita attraverso il servizio WSUW (Windows Server Update Service) è stata affiancata nel 2021 dallo strumento di software update integrato nel prodotto F-Secure. In questo modo è stato possibile distribuire aggiornamenti e patch non solo dei prodotti Microsoft, ma anche di quelli degli altri vendor. L'attività nel 2021 ha visto solo un gruppo selezionato di host che nel 2022 sarà esteso a a ulteriori personal computer.
  Parallelamente è stata avviata una fase di verifica dei server dotati di sistemi operativi non più supportati (soprattutto Windows server 2008 R2) programmandone la graduale sostituzione con versioni aggiornate.
- Anche l'attività di graduale sostituzione dei personal computer con sistema operativo Windows 7 è proseguita anche se permangono ancora circa 400 client da sostituire o aggiornare.
- Riduzione Servizi: nel 2021, anche a seguito di un progetto di collaborazione con il Politecnico di Torino è stata effettuata un'attività di monitoraggio del traffico di rete e di scansione dei servizi aperti, a seguito del quale si è provveduto a disattivare diversi servizi presenti su PC client che risultavano non non necessari.

5.4 rafforzamento dei controlli di sicurezza

Nel 2021 sono stati introdotti nuovi controlli di sicurezza e sono stati formalizzati alcune attività che prima venivano svolte senza una precisa schedulazione.
I controlli sono stati raccolti in apposite checklist a cadenza giornaliera, mensile e annuale e sono descritti nel documento "Organizzazione del servizio helpDesk, tecnico e sistemistico". Di cui si allega un estratto (controlli a carico del sistemista e controlli a carico dei tecnici).
Si cita in particolar modo il Task SSI002G.4 "Verifica EDR" che prevede l'analisi di tutte le segnalazioni classificate come rischio "Alto" e "Grave" presentate dal sistema di Endpoint Detection and Response. Tale sistema monitora l'ambiente IT ed in particolare i personal computer rilevando eventi e comportamenti che correlati fra loro possono ricondursi ad un malware. A differenza dei tradizionali sistemi di protezione basati su firme e indicatori di compromissione, può essere in grado di rilevare anche attacchi 0-day. La contropartita è la presenza di "falsi-positivi", ovvero di segnalazioni che non erano effettivamente riconducibili ad un'attività malevola ma, quasi sempre, ad attività dei tecnici di manutenzione.
Nel 2021 il sistema ha analizzato oltre 2 milioni di eventi rilevando circa 3500 segnalazioni di rischio "alto" e "grave", la cui analisi ha permesso di individuare e rimuovere dei malware nel due per cento dei casi.

5.5 Analisi criticità e individuazione ulteriori misure

L'attività di hardening ha permesso di individuare alcune criticità, soprattutto per quanto riguarda le utenze e i relativi privilegi. La riduzione dei privilegi amministrativi di dominio, che sarà completata nel 2022, è solo una parte. Sarebbe opportuno verificare anche i diritti assegnati agli utenti sui PC locali che, in passato, venivano impostati come "Power User".
Criticità ancora più rilevante è quella dell'utilizzo di account di reparto condivisi (es utortopedia, utlabanalisi, etc…). Tale comportamento, oltre a non essere conforme alle best practice di sicurezza informatica non è GDPR compliance. Sarebbe quindi opportuno eliminare tali utenze in favore dell'uso di quelle personali previo superamento del blocco dell'avvio del software di cartella clinica aziendale (BabeleWPF) la cui esecuzione viene impedita se sullo stesso PC è già aperta una sessione. Occorre inoltre considerare che sarà necessario un forte sostegno della direzione sanitaria perché l'iniziativa potrebbe incontrare delle resistenze da parte del personale che utilizzata tali utenze.
Anche l'attività di aggiornamento e patching dei software ha evidenziato alcune criticità essendo ancora presenti sistemi operativi server fuori supporto (Windows 2008 R2 e varie distribuzioni Linux). L'attività programmata nel 2022 dovrebbe sanare la situazione.
Parallelamente alle iniziative di cui sopra sono stati analizzati ulteriori strumenti che potrebbero aiutare a rafforzare le misure in tema di sicurezza informatica. In particolare:

- **Strumenti di formazione e simulazione di phishing.** Al fine di sensibilizzare maggiormente l'utenza sul problema degli attacchi via email, si è valutato che sarebbe di aiuto l'adozione di uno strumento di simulazione di phishing affiancato da brevi corsi di formazione automatizzata. Tra gli strumenti analizzati si cita "Sophos Phish Threat" che emula una vasta gamma di tipi di attacchi di phishing diversi, offre corsi di formazione integrati e permette di misurare il livello di sciurezza dell'organizzazione attraverso una reportistica completa. Sono in corso l'analisi di altri prodotti.
- **Security Email Gateway (SEG)**: una soluzione antispam, antimalware e di url rewrite per l'analisi all'interno di una sandbox dei link e degli allegati. La sua introduzione permetterebbe di ridurre le minacce via email che, oggi, costituisco il principale veicolo di attacco. Soprattutto la funzione di sandbox potrebbe permettere di sopperire ad eventuali comportamenti non corretti degli utenti che dovessero aprire link o allegati malevoli.
  Al momento sono stati valutati due prodotti: "Email Security" di Libra Esva e "Email Protection" di Proofpoint. Entrambe le soluzioni sono sembrate adeguate e nel 2022, previa analisi di ulteriori prodotti, verrà selezionato quello più adeguato.
- **Privileged Access Management (PAM)**: Un "accesso privilegiato" è un termine utilizzato per descrivere accessi o poteri speciali ben oltre quelli garantiti ad un utente standard, ad esempio gli amministratori del dominio. I sistemi PAM si basano sul principio dei privilegi minimi, che prevede che a ogni utente sia assegnato il livello minimo di accesso richiesto per svolgere le proprie mansioni. Il principio del privilegio minimo è ampiamente ritenuto una buona pratica per la sicurezza informatica ed è un passo fondamentale per proteggere gli accessi privilegiati a dati e risorse di massima criticità. L'applicazione del principio dei privilegi minimi consente alle organizzazioni di ridurre la superficie di attacco e mitigare i rischi portati da malintenzionati interni o cyber-attacchi esterni che possono causare violazioni dei dati estremamente dannose.
  L'introduzione di tale sistema potrebbe migliorare l'attività oggi effettuata manualmente senza l'ausilio di strumenti come questi.

- **Security Information and Event Management (SIEM).** Il SIEM è l'elemento che consente di raccogliere, archiviare, monitorare log e correlare eventi con l'obiettivo di identificare attacchi o violazioni di dati. Simile al sistema EDR già in uso che però raccoglie dati solo dai personal computer. Il SIEM, invece, colleziona i dati anche da server, apparati di rete, DB e Server Web. La sua introduzione, in affiancamento al sistema EDR o in sua sostituzione, potrebbe migliorare, in termini di tempestività e di numerosità, l'individuazione di compromissioni e di tentativi di attacco.
  Occorre comunque considerare che l'inserimento di tale strumento potrebbe avere impatto sull'iperatività del reparto IT richiedendo una gestione anche rilevante da parte di personale adeguatamente formato.
- **Security Orchestration, Automation and Response** (SOAR). Attraverso le piattaforme SOAR è possibile connettere i vasi strumenti di sicurezza permettendo l'automazione dei processi di sicurezza ripetibili e la risposta automatica a fronte di particolari eventi. Nel nostro contesto potrebbe essere utilizzata ad integrazione della piattaforma SIEM per automatizzare il processo di risposta nel processo di incident response.
  Da rilevare che questa tipologia di strumenti è utilizzata generalmente da SOC e CSIRT con una certa maturità che potrebbe non essere ancora stata raggiunta nella nostra realtà.
- **Secure WEB Gateway** (SWG). Strumento che offre le funzionalità di URL filtering, anti malware protection e di application control; Attualmente tali funzionalità sono coperte dal sistema Watchguard Total Security che però, come molti sistemi integrati all'interno dei next generation firewall, risulta meno flessibile rispetto a soluzioni dedicate. Lo strumento potrebbe eventualmente essere adottato in alternativa a quello attuale se ritenuto insufficiente dopo l'attività di revisione della configurazione.
- **Introduzione di server honeypot**. Gli honeypot sono dei sistemi hardware o software usati come "esca" per attirare i cyber criminali intenzionati ad attaccare il perimetro di sicurezza di un'organizzazione. L'idea è quella di predisporre due server virtuali (un file server e un db server) opportunamente configurati per ingannare eventuali attaccati e di tracciare connessioni di rete verso tali VM (non dovrebbero essere presenti), oltre a verificare l'accesso ai file e l'eventuale criptazione degli stessi. In alternativa potrebbero essere utilizzati soluzioni open source come Honeyd o HoneyC.

Si cita infine un tema che dovrà essere maggiormente approfondito nel 2022. Si tratta della strategia di gestione delle password e della loro scadenza. Infatti la regola, divenuta "universale", di obbligare gli utenti a cambiare le proprie password ogni 3-6 mesi nasce proprio nel 2003 dal National Institute of Standards and Technology.
Ma nel 2017 il NIST ha rivisto le proprie linee guida sulla gestione delle credenziali, rimuovendo la richiesta di cambio password periodico e aggiornando i requisiti di complessità. Questo è accaduto con la pubblicazione, a giugno 2017 dell'aggiornamento NIST SP 800-63 "Digital Identity Guidelines".
Le nuove linee guida emanate dal NIST, non cogenti in Europa ma comunque considerate un riferimento autorevole a livello mondiale. Sostengono che, obbligare arbitrariamente le persone a cambiare periodicamente le password (definite "memorized secrets") non è più considerata una pratica utile, anzi può portare l'utente ad utilizzare password banali per riuscire a ricordarle più facilmente (ogni volta che si è obbligati a cambiarle).
In altre parole, le politiche di scadenza delle password fanno più male che bene, perché inducono gli utenti ad impostare password molto prevedibili e strettamente correlate tra loro: quindi la password successiva può essere dedotta sulla base della password precedente.

Si aggiunge, tuttavia, che la password andrebbe comunque cambiata se c'è il sospetto o l'evidenza di una sua compromissione.
Questo tema dovrà essere oggetto di opportuna analisi nel 2022.

6. Conclusioni

La minaccia cibernetica cresce continuamente in quantità e qualità, determinata anche dall'evoluzione delle tecniche di ingegneria sociale volte a ingannare gli utenti finali dei servizi digitali sia interni che fruitori dall'esterno.
Inoltre, si assistite ad un incremento notevole degli attacchi. È necessario quindi un cambio di approccio in cui la cybersecurity non deve essere vista come un costo o un mero adempimento normativo ma come un'opportunità per la crescita e la trasformazione digitale.
Il personale della S.C. Sistemi Informativi ha abbracciato tale filosofia e consapevole delle difficoltà ha avviato un percorso di rafforzamento e crescita con obiettivi ambiziosi.

Allegati

Valutazione Conoscenze Cybersecurity.pdf

Controlli a carico del sistemista

Controlli a carico dei tecnici

Controlli a carico del sistemista

Periodicità	idTask	Task	Descrizione	Outcome
(cadenza e periodo suggerito per lo svolgimento attività)				
Giornaliera (prima mattina)	1	Verifica esito backup	Verifica esito Backup Terarecon (mail a manutenzione delle ore 20.30) Verifica HL7 Backup ARCLOG e Dump Oracle giorno precedente Verifica Backup Veeam CSI (da mail) Verifica Backup Simpana	Solo in caso di fallimenti segnalare via email le azione intraprese
Giornaliera (attività continuativa durante durante orario lavorativo)	2	Monitoraggio attraverso Check MK	Monitorare durante la giornata lavorativa lo stato delle risorse attraverso l'apposita console predisposta su Check MK	Solo in caso di segnalazioni rilevanti inviare rapporto via email
Giornaliera (attività continuativa durante durante orario lavorativo)	3	Monitoraggio con sherlogic	Monitorare durante la giornata lavorativa eventuali alert del programma.	Solo in caso di segnalazioni rilevanti inviare rapporto via email
Settimanale	4	Verifica comunicazione AD	Controlli standard su DC e sincronizzazione	Scheda SSI003M
Mensile (fine mese)	5	Aggiornamento server Sql	Verifica ed eventuale aggiornamento OS, server: DWH2S05B DWH2S01 SANI2S07B SANI2S03	Scheda SSI003M
Mensile (metà mese)	6	Verifica traffico DNS verso IP non corretti	Verifica con wireshark di traffico anomalo DNS verso gli IP interni che non sono corretti	Scheda SSI003M + email con evidenze
Trimestrale	7	Aggiornamento scheda Server Fisici e VM	Aggiornamento scheda elenco server Verifica eventi significativi su log server (event viewer per Windows) Verifica spazio residuo su file system ed eventuali estensioni Verifica/installazione aggiornamenti OS.	Scheda SSI005A + Report Server da depositare in Area_CED_Tecnici\Server
Semestrale	8	Verifica Volumi storage	Verifica degli storage e del relativo spazio occupato/disponibile	Scheda SSI005A + Report Storage da depositare in Area_CED_Tecnici\Storage
Semestrale	9	Verifica aggiornamento Hypervisor	Verifica ed installazione patch ed aggiornamenti infrastruttura di virtualizzazione	Email + Scheda SSI005A
Annuale	10	Verifica aggiornamenti firmware	Verifica e installazione aggiornamenti firmware host fisici Verifica e installazione aggiornamenti firmware storage	Email + Scheda SSI005A

Controlli a carico dei tecnici

Periodicità / Incaricato	idTask	Task	Descrizione	Outcome
(cadenza e periodo suggerito per lo svolgimento attività e soggetto incaricato)				
Giornaliera ore 8:00 Morella (in sua assenza Lari)	1	Verifica esito backup	Verifica esito Backup Terarecon (mail a manutenzione delle ore 20.30) Verifica HL7 Backup ARCLOG e Dump Oracle giorno precedente Verifica Backup Veeam CSI (da mail) Verifica Backup Simpana	Scheda SSI002G
Giornaliera Lari (in sua assenza Morella)	2	Verifica alert antivirus	Da console F-Secure – spostarsi su root e verificare segnalazioni alert giorni precedenti. Intraprendere le opportune azioni come da procedura.	Scheda SSI002G
Giornaliera Lari (in sua assenza Morella)	3	Verifica presenza installazioni antivirus	Da console F-Secure - Autodiscover Windows Host con flag “Hide alredu manged hosts” selezionato. Eventuali host senza AV dovranno essere: => segnalati ad Emiliano se server => gestiti se client	Scheda SSI002G
Giornaliera Morella (in sua assenza Lari)	4	Verifica EDR	Verificare tutte le segnalazioni a richio Alto e Grave. Approfondire coinvolgendo dove necessario il sistemista. Registrare la chiusura una volta gestite.	Scheda SSI002G
Mensile (inizio mese) Lari	5	Verifica Utenti AD attivi	- Estrarre elenco utenti AD attivi con query powershell e verificare gli utenti che non accedono da oltre 1 anno. valutare se disabilitare => N.B.: su quelli da NON disabilitare inserire un commento esplicito che giustifichi il mantenimento allo stato attivo -Confrontare elenco attivi con elenco degli utenti cessati (da estrazione Sql) e valutare disabilitazione ==> N.B.: su quelli da NON disabilitare inserire un commento esplicito che giustifichi il manutenimento allo stato attivo -Estrarre da Sql gli utenti cessati negli ultimi 2 mesi e verificare che siano stati disattivati su AD o in alternativa che siano giustificati ad operare	Scheda SSI004M + email con risultati attività
Semestrale (maggio,novembre) Morella	6	Verifica PC AD Attivi	Estrarre elenco PC AD attivi con query powershell e confrontare con elenco sysaid, DHCP e file ipaddres => procedere con le opportune disabilitazioni	Scheda SSI004M + email con risultati attività
Mensile (inizio mese) Morella	7	Manutenzione Server DHCP	Verifica lease duplicate	Scheda SSI004M + email con risultati attività
Mensile (inizio mese) (Catoggio)	8	Verifica PC che non comunicano con agent Sysaid	Elenco Asset, applicare advanced filter “Fonte è agente e disabilitato e No e Ora aggiornamento è minore di 1/1/2021” (usare una data pari a circa 6 mesi prima) quindi gestire tutti record risultanti. Dove necessario aprire ticket ai tecnici per reinstallazione Agent	Scheda SSI004M
Mensile (metà mese) (Catoggio)	9	Verifica su Sysaid degli asset senza inventario	Elenco Asset, applicare advanced filtro “inventario 1 È vuoto” quindi gestire tutte i recod risultanti: effettuare le opportune verifiche eliminando i record errati o inserendo l’apposito inventario	Scheda SSI004M
Giornaliera ore 8:15 Lari (in sua assenza Morella)	10	Cambio cassette DAT Fondazione		Scheda SSI002G

Periodicità / Incaricato	**idTask**	**Task**	**Descrizione**	**Outcome**
(cadenza e periodo suggerito per lo svolgimento attività e soggetto incaricato)				
Giornaliera ore 8:00 Lari (in sua assenza Morella)	11	Verifica visiva spie sala server (ORE		Scheda SSI002G
Giornaliera ore 8:00 Morella (in sua assenza Lari)	12	Query monitoraggio		Scheda SSI002G
Giornaliera ore 8:00 Morella (in sua assenza Lari)	13	Verifica FTP timbrature mensa	Occorre verificare all'interno del file \\ssi2s12\ Area_Boll\log che nella giornata corrente sia stato trasferito il file transaz_mensa.dat (nel log deve risultare il trasferimento di x bytes (con x >0)	Scheda SSI002G