Sede legale: Via Magellano, 1 - 10128 TORINO - Tel. +39 011.508.1111 - www.mauriziano.it - P.I./Cod. Fisc. 09059340019

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

Relazione sulle misure in tema di cybersecurity

Relazione di riepilogo Anno 2022

aggiornamento rispetto all'anno 2021

Indice generale

1. Premessa

Il presente documento costituisce un aggiornamento della precedente relazione **"**Relazione sulle misure in tema di cybersecurity" dell'anno 2021 (pubblicata sul sito all'indirizzo https://www.mauriziano.it/flex/cm/pages/ServeBLOB.php/L/IT/IDPagina/964), che ne costituisce una parte integrante. Molti aspetti che sono rimasti senza significative modifiche, come la normativa di riferimento, l'organizzazione del personale addetto alla cybersecurity e le misure di sicurezza implementate, non saranno ripresi nel presente documento.

2. Il contesto di riferimento nel 2022

Nel nostro paese si conferma il trend crescente di attacchi, già rilevato negli anni precedenti. In particolare nel I semestre 2022 vediamo un incremento dell'8,4% rispetto allo stesso periodo dell'anno precedente (fonte rapporto Clusit 2022).
Il settore sanitario rimane tra i bersagli privilegiati dai cyber criminali, mossi soprattutto dalla particolare rilevanza e riservatezza dei dati che vi transitano e che, ovviamente, generano un grande valore economico.
Fra i molti attacchi vanno richiamati i casi dell'ULSS 6 Euganea, dell'ospedale milanese Fatebenefratelli e dell'ASL Città di Torino, nei quali le conseguenze si sono tradotte in significativi ritardi (o addirittura interruzioni) dei servizi ai pazienti.
In totale nei primi sei mesi del 2022 la sanità ha subito 630 eventi critici ovvero attività gravi in termini di rischio e di impatto sull'infrastruttura digitale dell'organizzazione (fonte infosec.new).
Per quanto riguarda le tipologie di attacco al primo posto rimane il ransomware, ormai da tempo la famiglia di malware più diffusa e per cui l'Italia detiene il primato negativo in Europa.
In misura minore, ma con aumenti considerevoli rispetto all'anno precedente, continuano a osservarsi anche attacchi di tipo DDoS (+308,8%) e attività di phishing/social engineering (+63,8%) finalizzate a carpire credenziali con cui poter, poi, compiere gli attacchi veri e propri.
Tra i fattori che hanno contribuito all'aumento degli attacchi vi è sicuramente il conflitto russo-ucraino che ha determinato anche una caratterizzazione del tipo di attacchi.

3. La situazione aziendale

Per quanto riguarda la situazione della nostra azienda si segnala che nel corso del 2022 non sono stati rilevati attacchi di rilievo che abbiano avuto successo.
In generale è stata osservata una intensificazione dei tentativi di phishing e di spear phishing, contraddistinti, in molti casi, da email con testi sempre più accurati, scritti in italiano corretto, e con un linguaggio tale da rendere, a prima vista, più complesso il riconoscimento della minaccia.
Tale situazione è stata calmierata grazie ad una maggior consapevolezza in tema di cybersecurity da parte degli utenti, frutto anche delle iniziative di sensibilizzazione intraprese dalla nostra struttura nel corso degli ultimi anni . Inoltre, proprio grazie alle pronte segnalazioni del personale più attento, è stato possibile configurare sul server email aziendale delle regole di filtering per specifiche campagne di phishing, limitando parzialmente la diffusione delle email malevoli.

4. Iniziative intraprese nel 2022 e attività programmate nel 2023

La posta elettronica rimane, comunque uno dei principali vettori, per i malware e per questo motivo l'azienda nel 2022 ha aderito all'accordo quadro "Cybersecurity - prodotti e servizi connessi" e attraverso l' RDO n. 3259089 ha avviato la procedura di rilancio competitivo per l'acquisizione di

un sistema di Secure Email Gateway (SEG), aggiudicando in data 28/11/2002 il prodotto LIBRAESVA offerto dalla Telecom.

L'installazione e configurazione del SEG è stata programmata nel mese di gennaio 2023 e prevede l'installazione di due appliance virtuali a protezione del traffico email.
Grazie a questo sistema sarà possibile proteggersi in maniera più efficace contro Malware, Phishing, Ransomware, URL e allegati dannosi, compromissione delle e-mail aziendali (BEC) e altre tipologia di attacco.

In linea con l'approccio continuo ed iterativo basato sul modello Plan-Do-Check-Act, nel 2022 è proseguita l'attività di individuazione, valutazione, trattamento e documentazione dei rischi associati alla gestione dei sistemi e delle infrastrutture informatiche, da cui poi scaturiscono molte delle iniziative di intervento.
Nel 2023 proseguiranno tali azioni con particolare attenzioni all'attività di hardering volta a ridurre la superficie e le vulnerabilità che posso essere sfruttate per un attacco.
Proseguiranno in particolar modo:

- La revisione delle regole del firewall con chiusura delle porte non necessarie.
- La disabilitazione utenti inattivi: si tratta della disattivazione degli utenti che hanno cessato il loro rapporto di lavoro o di collaborazione con l'azienda.
- La 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'aggiornamento software e installazione patch di sicurezza: l'attività di aggiornamento "ordinaria" eseguita attraverso il servizio WSUS (Windows Server Update Service) e lo strumento di software update integrato nel prodotto With-Secure. In particolare, per quest'ultimo prodotto, nel 2022 abbiamo esteso in maniera significativa il perimetro dei PC e dei software oggetto di aggiornamento automatico.
- La sostituzione/eliminazione di server dotati di sistemi operativi non più supportati (soprattutto Windows server 2008 R2). Sebbene nel 2022 siano stati migrati molti servizi, ne rimangono ancora alcuni da migrare e che permetteranno il proseguimento dell'attività
- La sostituzione dei personal computer con sistema operativo Windows 7 e 8. Nel 2022 sono stati sostituiti/aggiornati circa 250 client. Il completamento dei restanti 160 è prevista nel 2023.

Oltre alle attività di hardering sopra descritta si citano alcuni progetti specifici, quali:

- Analisi Sostituzione dei firewall: a seguito della scadenza dei servizi della suite Watchguard Total Security è stato previsto che nel corso del anno venturo saranno esaminati eventuali prodotti alternativi che possano presentare adeguati livelli di sicurezza e che superino alcuni dei limiti di usabilità rilevati sugli attuali strumenti.
- Ricerca di un prodotto SIEM (Security Information and Event Management). Nel 2022 sono state valutate alcune soluzioni che non erano conformi ai vincoli di budget (es. Darktrace) o che presentavano una complessità di gestione tale da richiedere personale dedicato allo scopo (es. FortiSIEM di Fortigate e Qradar di IBM). Nel 2023 proseguiranno gli approfondimenti volti a selezionare il prodotto più adeguato al contesto aziendale.

- Proseguo delle iniziative di CyberSecurity Awareness volte a misurare ed aumentare la consapevolezza del rischio cyber, prevedendo l'introduzione di alcuni questionari e dei test di phishing.

Da citare inoltre il rafforzamento dei sistemi di Disaster Recovery (DR) che, pur non costituendo uno strumento di prevenzione degli attacchi, potrà aiutare a garantire l'affidabilità dei sistemi e a rispondere in modo adeguato e tempestivo ad eventuali incidenti.
Tra questi va sicuramente citato il progetto di replica dei db aziendali su sito esterno (server farm Nivola del CSI) la cui realizzazione è prevista nel corso del prossimo anno.
Parallelamente saranno avviati alcuni approfondimenti per la replica anche dell'ambiente applicativo (cartella clinica) o almeno di una parte delle funzionalità affinché siano disponibili anche da postazioni remotizzate attraverso soluzioni di desktop remoto.

Gli approfondimenti in merito alla direttiva NIST SP 800-63 "Digital Identity Guidelines" e all'opportunità di modifica dei criteri di scadenza delle password, previsti inizialmente nel 2022 saranno oggetto di approfondimento nel 2023.

5. Conclusioni

La minaccia cibernetica cresce continuamente e nel settore sanitario gli impatti hanno conseguenze molto più gravi che in altri settori. Secondo uno studio di Ponemon Institute, una delle principali organizzazioni di ricerca sulla sicurezza informatica, e di Proofpoint Inc, azienda leader nel settore della cybersecurity e della compliance, oltre il 20% delle organizzazioni in ambito sanitario ha subito considerevoli perdite economiche e, cosa ancor più grave, ha visto crescere il tasso di mortalità a causa di ritardi nelle procedure e negli esami.
Tra i principali aspetti emersi nel report si citano due aspetti di rilievo:

- I programmi di formazione e sensibilizzazione, insieme al monitoraggio dei dipendenti, rappresentano una delle principali difese
- La mancanza di fondi e risorse (soprattutto in termini di competenze interne e personale preposto all'attività) rappresentare una criticità

Tutto ciò obbliga le aziende del nostro settore a dover rafforzare le misure di sicurezza, allocando le necessarie risorse e coinvolgendo in maniera attiva tutto il personale dell'azienda.

Torino, 11 gennaio 2023

Dr. Stefano Geninatti Togli