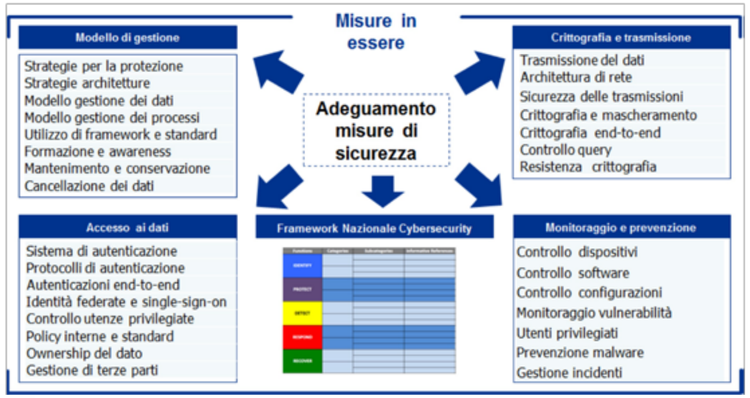
laboratorio SANITÀ 2030 LOMBARDIA
14-15 GIUGNO 2023
FIERA DI BERGAMO

Gruppo San Donato

Gianluca CAVALLETTI
Global Chief Information Officer & Chief Information Security Officer
President & CEO – Wennovia (GSD)
Chief Information Officer - San Raffaele Hospital –
Professor (a.c.) Information Technology , Vita & Salute University (San Raffaele)

La normativa NIS indirizza puntualmente le misure tecniche e organizzative che gli OSE devono mettere in atto per prevenire e minimizzare l'impatto degli incidenti a carico della sicurezza delle reti e dei sistemi informativi.
Inoltre, per ciò che riguarda il GDPR e per la tipologia di dati trattati, si dovrà procedere ad aggiornare costantemente l'Analisi dei Rischi e la Valutazione d'Impatto sui dati trattati con un adeguato coordinamento tra DPO e IT Security.
Su tale base documentale si dovrà poi procedere al periodico adeguamento delle misure di sicurezza di Gruppo.



Gruppo San Donato

laboratorio SANITÀ 2030™
14-15 GIUGNO 2023 LOMBARDIA
FIERA DI BERGAMO

Un programma di protezione complesso e articolato che ogni azienda ospedaliere deve affrontare, ha come obbiettivo la mitigazione consistente tutti gli attacchi derivanti dal Cyber Crime.
I cyber attacchi possono provocare gravissimi danni operativi alle strutture ospedaliere e conseguentemente impatti economici non quantificabili poiché «ampi a piacere» e potenzialmente **senza limiti**.

Da Rapporto Clusit - Associazione Italiana per la Sicurezza Informatica: «*Cybersecurity - In Italia c'è un attacco grave ogni 5 ore. Più 91,2% in 5 anni - Un quarto degli attacchi è stato portato in parallelo verso "bersagli multipli": **in un anno sono cresciuti del 91,5% gli attacchi a servizi online e del 17% quelli alla sanità**. Aumento esponenziale (+81,9%) anche per le tecniche di "phishing" e "social engineering"*

A titolo esemplificativo, ma non esaustivo, un programma di protezione a 360 gradi consente di **mitigare il rischio di attacchi con gravi impatti economici** dovuti a:

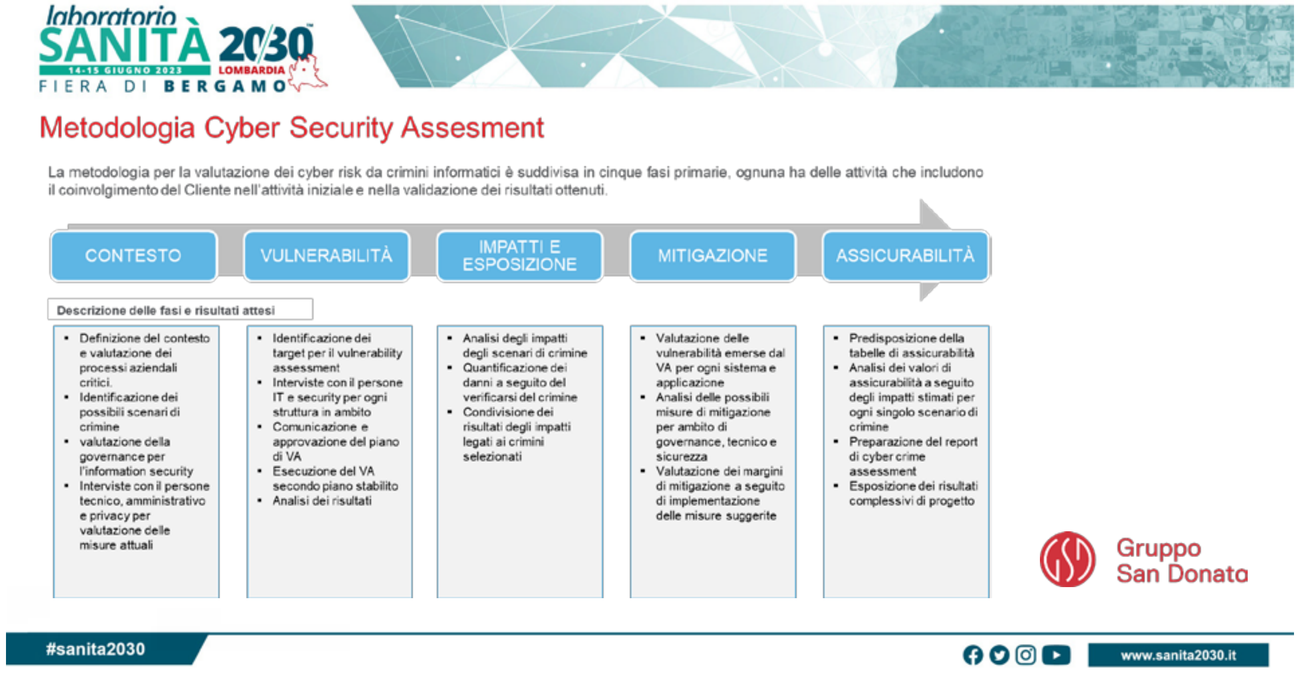
Azioni malevole dirette con impatti sulla produttività
- Crimini volti a minare la corretta attività degli ospedali, attraverso la generazione di disfunzioni gravi, con impatto diretto sui costi operativi. Danni da lucro cessante e sulla produttività complessiva. Incapacità di poter assolvere a tutte le funzioni e servizi amministrativi e clinici.

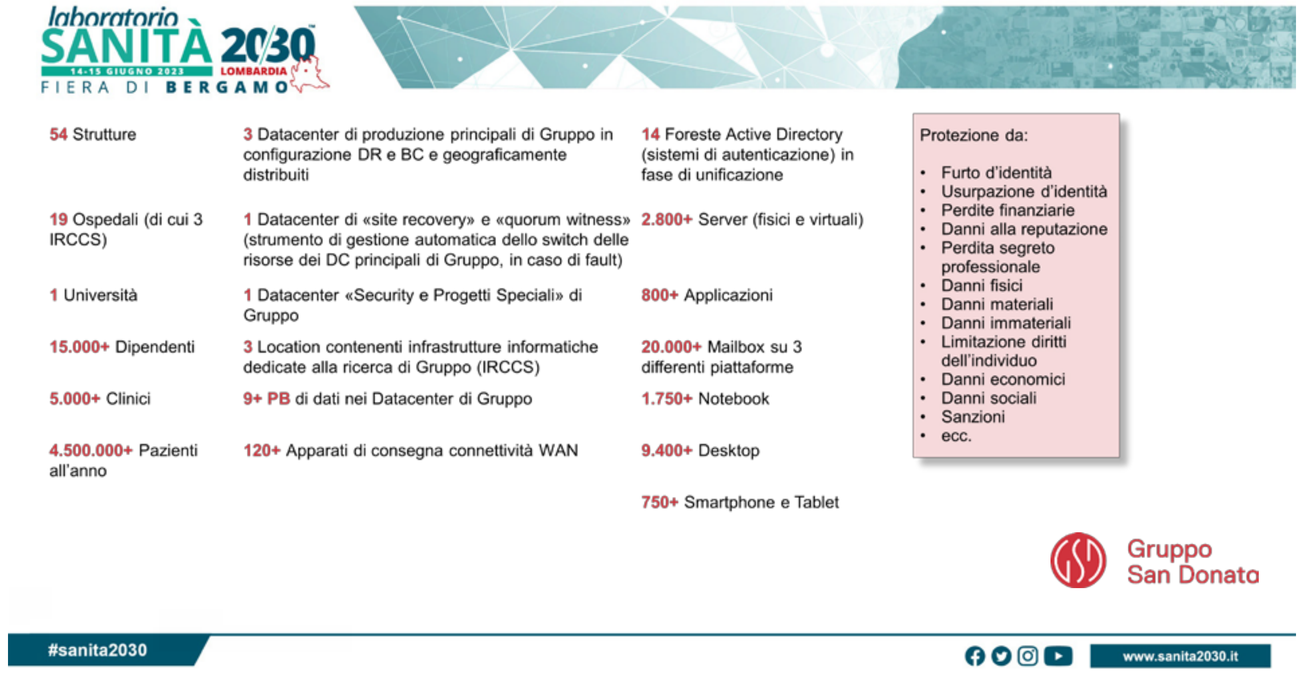
Azioni malevole con impatti sul servizio al paziente
- Attacchi a mezzo di virus (ad esempio «ransomware» finalizzati all'estorsione di denaro), con impatti sull'operatività e, nei casi più gravi, con possibili ripercussioni sulla salute dei pazienti
- Impossibilità di curare adeguatamente i pazienti

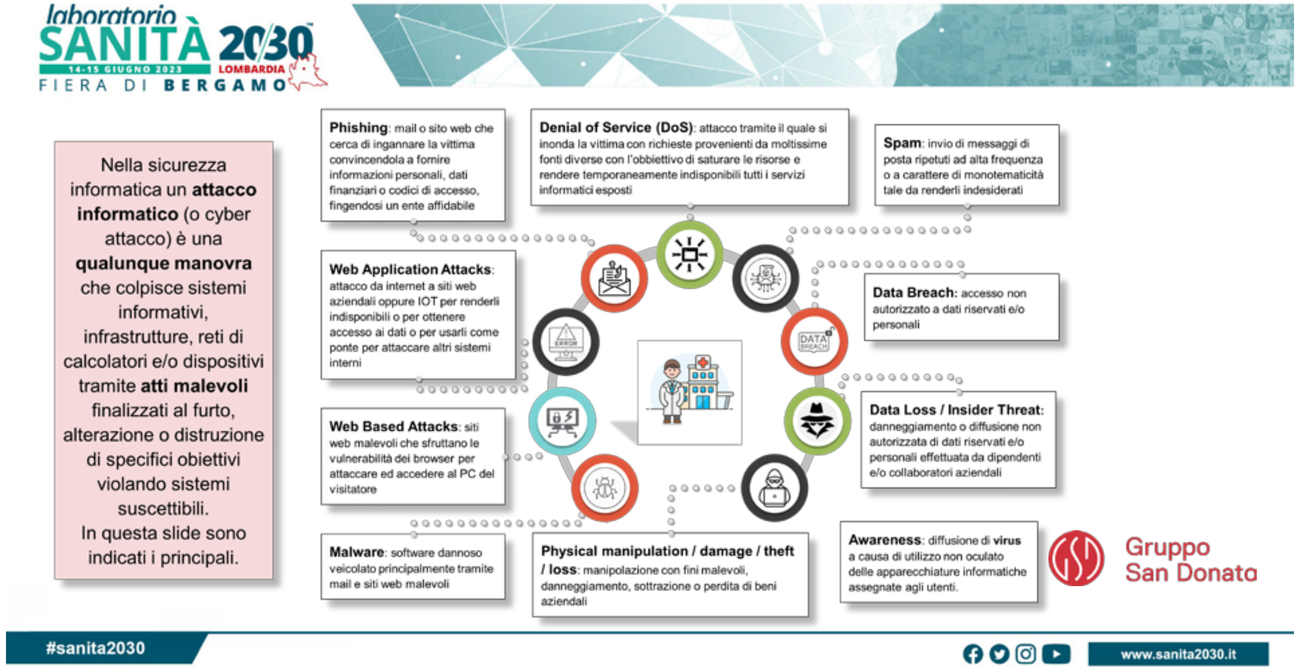
Azioni malevole dirette verso i dati clinici e di business:
- Esfiltrazione di dati personali e sensibili, con conseguenti cause di risarcimento danni da parte degli interessati e con sanzioni da parte del GDPR (che possono arrivare fino al 4% del fatturato dell'Organizzazione)
- Modifica o cancellazione del dato con impatti sulla salute del paziente, referti e parametri vitali modificati, percorsi di cura e somministrazioni farmacologiche alterate
- Modifica dei parametri di funzionamento degli apparati elettromedicali con intenti malevoli (es modifica dei parametri di irraggiamento, modifica della funzionalità di strumentazioni cliniche)
- Truffe assicurative
- Spionaggio industriale (es. ricerca) e sabotaggio con appropriazione anche di dati economici finanziari e/o operazioni di mercato.
- Frodi interne finalizzate al lucro criminale o al sabotaggio dell'organizzazione

Conseguenze generali :
- Danni ai pazienti sia in termini economici (contenziosi) , che di salute (anche alla vita)
- Danni economici di natura sanzionatoria e risarcitoria
- Danni economici per estorsione/ricatto
- Danni di immagine/reputazione

Gruppo San Donato







Le cinque fasi che, di solito, un organizzazione professionale di hacker segue per introdursi in un sistema aziendale sono:

1. **RICOGNIZIONE** - La fase di ricognizione si riferisce a quel momento di preparazione iniziale in cui i cybercriminali raccolgono quante più informazioni possibili sull'obiettivo per definire la strategia di attacco.

2. **SCANSIONE** - La scansione è l'azione che i cybercriminali eseguono prima di attaccare. Nella scansione, usano i dettagli raccolti durante le ricognizioni per identificare le specifiche vulnerabilità. Spesso vengono utilizzati strumenti automatizzati come scanner di rete/host e war-dialer per individuare i sistemi e tentare di scoprirne le vulnerabilità.

3. **OTTENIMENTO DELL'ACCESSO** – L'accesso ai sistemi è la fase più importante di un attacco (in termini di danno potenziale) dopo averne scoperto le vulnerabilità tramite la scansione. N.B. I cybercriminali non hanno sempre bisogno di ottenere l'accesso al sistema per causare danni. Gli attacchi Denial-of-Service (DoS), ad esempio, possono esaurire le risorse o interrompere i servizi di esecuzione sul sistema di destinazione.

4. **MANTENIMENTO DELL'ACCESSO** - Una volta che i cybercriminali ottengono l'accesso al sistema di destinazione, possono scegliere di utilizzare il sistema e le sue risorse come trampolino di lancio per scansionare e sfruttare altri sistemi, oppure scegliere di mantenere un «profilo basso» e continuare a sfruttare esclusivamente quel singolo sistema.

5. **COPERTURA TRACCE** - I cybercriminali di solito distruggono le prove della loro presenza ed attività. Cancellare le prove di un attacco è un requisito essenziale per qualsiasi cybercriminale che vuole rimanere inosservato (ed impunito). Di solito questa fase inizia con la cancellazione degli accessi e di eventuali messaggi di errore che potrebbero essere stati generati dal processo di attacco. Successivamente l'attenzione è di solito rivolta a modificare i parametri di sistema in modo che gli accessi futuri non vengano più registrati.

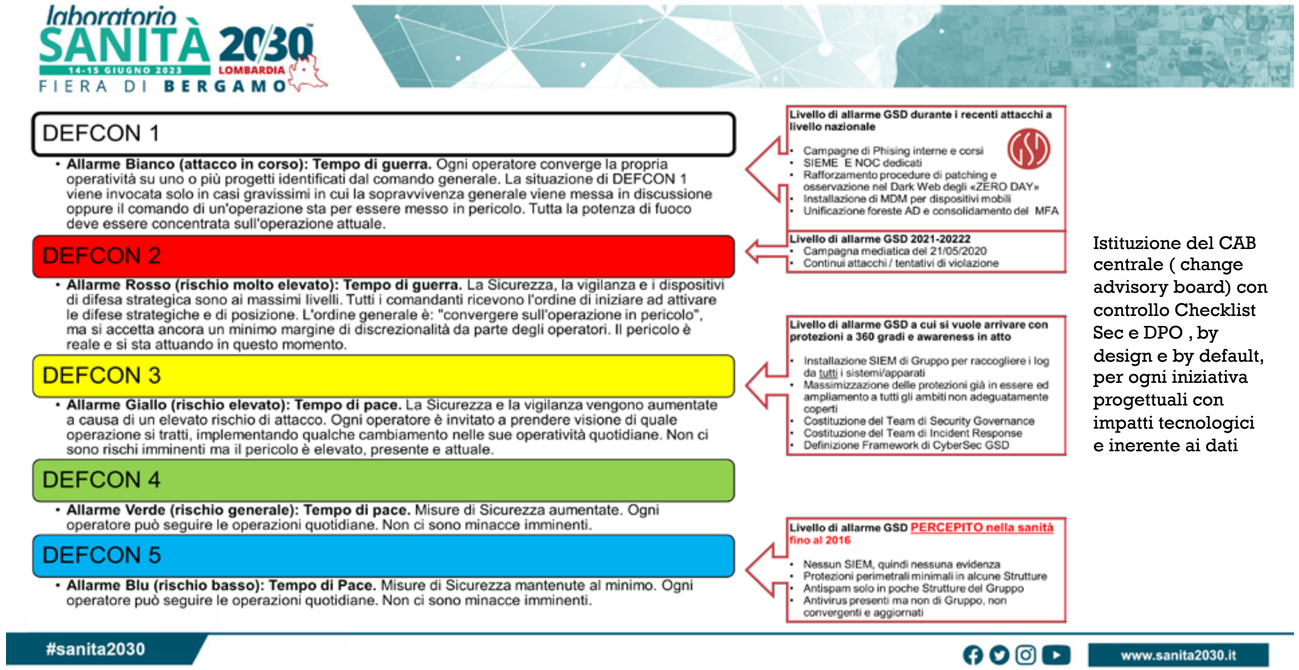
Gruppo San Donato

Tipo Utente/ Tipo Attacco	Malware (1)	Webased Attacks (1)	WebApp Attacks (1)	Phishing (1)	Spam (1)	Data Breaches (1)	Physical (1)	DL / Insider Threat (2)
Utenti standard	media	media	n.d.	media	bassa	media	media	media
Utenti VIP / Admin	alta	alta	n.d.	alta	bassa	alta	alta	alta
Medici / Operatori	alta	alta	n.d.	alta	bassa	alta	alta	alta
Pazienti	bassa	bassa	n.d.	bassa	bassa	bassa	bassa	bassa
Sistemi Università	media	n.d.	media	n.d.	n.d.	media	media	n.d.
Sistemi Ricerca	alta	n.d.	alta	n.d.	n.d.	alta	media	n.d.
Sistemi Ing. Clinica	alta	n.d.	alta	n.d.	n.d.	alta	alta	n.d.
Sistemi IT	alta	n.d.	alta	n.d.	n.d.	alta	alta	n.d.

(1) La criticità è riferita al caso in cui persone o sistemi appartenenti alla categoria indicata subiscano il tipo di attacco indicato (caso peggiore)
(2) La criticità è riferita al caso in cui persone appartenenti alla categoria indicata effettuino il tipo di attacco indicato (caso peggiore)

Gruppo San Donato

#sanita2030 www.sanita2030.it



Istituzione del CAB centrale (change advisory board) con controllo Checklist Sec e DPO , by design e by default, per ogni iniziativa progettuali con impatti tecnologici e inerente ai dati

NUOVI FIREWALL DI GRUPPO

La nuova rete d'interconnessione ha permesso **l'ottimizzazione degli accessi ad internet** che si sono potuti far convergere nei due nuovi datacenter (ad esclusione degli accessi al GARR che devono continuare ad essere collegati direttamente alle Strutture che ne hanno titolo) dove sono stati installati due nuovi firewall di classe enterprise che regolano e proteggono il traffico tra tutte le Strutture del Gruppo ed Internet.

Ambiti di protezione: **Denial of Service** (per attacchi DDoS di piccola o media entità), **Web Application Attacks** (tramite le funzionalità di IPS/IDS), **Web Based Attacks** (tramite le funzionalità di Url Filtering)

I «Firewall a Segmentazione» servono ad introdurre un ulteriore grado di protezione, essendo in grado sia di proteggere da attacchi provenienti «dall'esterno» del perimetro di ciascuna Struttura che di creare zone segregate all'interno delle stesse, per cui l'attacco portato a segno ad un sistema informatico (es. un elettromedicale) non si propaghi al di fuori della zona di appartenenza (VLAN).

NUOVI APPARATI ANTISPAM

Gli Antispam, installati all'interno dei due nuovi datacenter di Gruppo, **attenuano** il fenomeno della **posta indesiderata** e **proteggono il servizio mail on premises** (e di conseguenza anche la rete aziendale) limitando la propagazione di software malevolo. Attualmente a protezione di una parte delle caselle di posta GSD (es. VIP).

Ambiti di protezione: **Spam** (tramite valutazione della reputazione del mittente), **Phishing** (tramite analisi del testo e link presenti nella mail), **Malware** (tramite analisi degli allegati)

Gruppo San Donato

laboratorio SANITÀ 2030™
14-15 GIUGNO 2023 LOMBARDIA
FIERA DI BERGAMO

NUOVA RETE D'INTERCONNESSIONE DI GRUPPO

La nuova rete MPLS di Gruppo oltre a garantire elevatissime performance, ha permesso l'**eliminazione della maggior parte dei Single Point Of Failure** (SPoF) presenti, come ad esempio:

- *connessioni non ridondate*: la continuità di servizio non era garantita in caso di malfunzionamento dell'unica linea esistente
- *connessioni VPN su canale pubblico per sopperire alla mancanza di linee dedicate*: il canale internet non offre le stesse garanzie di banda e di resilienza di una MPLS dedicata e ridondata
- *percorsi di rete non ottimizzati*: tutte le connessioni sono stati razionalizzate, eliminando le "relazioni uno-a-molti" che rendevano difficile analizzare e gestire le problematiche nel colloquio di rete tra le Strutture del Gruppo.

Ambiti di protezione: **Denial of Service (DoS), Data Breach, Malware, Awareness** (grazie ad una rete d'interconnessione ottimizzata e completamente dedicata, e con l'unificazione dei percorsi di accesso a Internet, si riducono i possibili punti di attacco)

Gruppo San Donato

INSTALLAZIONE STRUMENTI PER ANALISI SICUREZZA

Ogni giorno nascono nuove minacce ed è quindi importante **verificare periodicamente** tutti i sistemi informatici sulla base delle più recenti vulnerabilità note.

Per questo motivo il team IT Security si è dotato di due prodotti «leader» pensati per questo tipo di verifiche atte a :

- effettuare **Vulnerability Assessment**
  Il Vulnerability Assessment è un vero e proprio check-up dei sistemi informatici, una sorta di scanning che mira a far emergere possibili vulnerabilità dell'infrastruttura e della rete IT. Lo scopo è quello di identificare quali parti del sistema risultino deboli a livello di sicurezza per poi stilare un Remediation Plan.
- effettuare **Penetration Test.**
  Il Penetration Test è una simulazione di attacco verso un determinato obiettivo per testare l'efficacia delle difese che un hacker potrebbe voler bypassare. Permette quindi di avere conferma dell'esistenza o meno di una o più vulnerabilità e, cosa più importante, di determinarne le conseguenze nel caso di un eventuale attacco reale.

Nota: Questi strumenti permettono anche di verificare in autonomia la «Security by Design» di ogni nuovo rilascio applicativo o sistemistico.

SERVIZIO SOC-SIEM Il Servizio, attivo dall'inizio del 2020, ha lo scopo **collezionare ed analizzare** (*SIEM, Security Information and Event Management*) e di **segnalare** (*SOC, Security Operation Center*) **comportamenti anomali** di sistemi/persone tramite l'analisi e la **correlazione di informazioni** provenienti da alcune fonti (e.g. accesso e/o operazioni malevoli su apparati) così da **individuare anomalie** all'interno del traffico di rete e quindi eventuali problemi di sicurezza.

Gruppo San Donato

NUOVI DATACENTER (MIGRAZIONE SISTEMI)

I nuovi Datacenter, all'interno dei quali sono confluti i sistemi e i dati presenti negli precedenti 14 «data center» delle Strutture del Gruppo San Donato, sono certificati TIER 3 e TIER 4 e assicurano una **altissima disponibilità operativa** in termini di continuità elettrica, climatizzazione e sistemi di controllo ambientale (ad esempio umidità dell'aria, fumi, sistemi antincendio).

Garantiscono inoltre la sicurezza fisica di tutti gli apparati presenti contro furto o danneggiamento, in quanto questi sono protetti da "cage" e sono attuate **rigorose procedure** di **autorizzazione** all'accesso ed **identificazione** delle persone.

Per i sistemi Cloud ready è in corso migrazione su sistemi ibridi

Ambiti di protezione: **Physical manipulation / damage / theft / loss, Data Breach, Data Loss / Insider Threat**

SOLUZIONI NAC (NETWORK ACCESS CONTROL) NELLE STRUTTURE

Gli obiettivi principali dei NAC sono autorizzare, autenticare e fare l'accounting delle connessioni di rete, rafforzare il controllo di identità e gestione degli accessi, mitigando la possibilità di attacchi dall'interno della rete aziendale: i dispositivi non potranno connettersi alla rete fintanto che non rispettano policy di sicurezza (o compliance) predefinite.

Grazie alle soluzioni, già presenti nel Gruppo, sono state implementate le regole di NAC all'interno delle strutture più esposte.

Ambiti di protezione: **Denial of Service (DoS), Malware, Data Breach, Data Loss / Insider Threat, Awareness**

Gruppo San Donato

laboratorio SANITÀ 2030 LOMBARDIA
14-15 GIUGNO 2023
FIERA DI BERGAMO

WIFI DI GRUPPO evoluti e controllate (anche per BYOD)

Il progetto «**WIFI di Gruppo**» permette di avere la *copertura totale Wi-Fi* (100% di tutte le aree interne agli edifici) e la *copertura totale con tecnologia Beacon Bluetooth* di tutte le Strutture del Gruppo San Donato.

Il progetto ha anche l'obbiettivo di creare un ecosistema che consenta di localizzare tutte le «entità» all'interno delle Strutture e di consentire **l'accesso sicuro e controllato alla rete**, da qualsiasi device mobile, agli operatori del Gruppo, ai pazienti e visitatori.

Anche per le reti WIFI valgono le stesse considerazioni fatte per la segmentazione della rete fisica: la **creazione di nomi di accesso diversi** e separati tra loro (SSID) e i controlli di sicurezza (grazie ai WLC ed ai firewall interni) hanno lo scopo di **confinare** un eventuale **problema** (es. la diffusione di malware o il raggio d'azione di un aggressore penetrato in una falla della rete) nel segmento della rete dove si è verificato, evitando di minacciare gli altri.

Ambiti di protezione: **Denial of Service (DoS), Malware, Data Breach, Data Loss / Insider Threat, Awareness**

Gruppo San Donato

#sanita2030

www.sanita2030.it

laboratorio SANITÀ 2030™
14-15 GIUGNO 2023 LOMBARDIA
FIERA DI BERGAMO

IMPLEMENTAZIONE SISTEMA PAM

Il **progetto PAM** (Privileged Access Management) consiste nell'introduzione di una classe di soluzioni che aiutano a **proteggere**, **controllare**, **gestire** e **monitorare** l'accesso privilegiato ai sistemi critici sia da parte del *personale interno* (e.g. sistemisti, sviluppatori, ecc.) che da parte dei *fornitori* del Gruppo San Donato (e.g: gestione applicativa, troubleshooting, ecc.).

Centralizzando la gestione delle credenziali privilegiate e la loro distribuzione in un unico punto, i sistemi PAM possono quindi **garantire** un elevato livello di sicurezza, **controllare** chi li sta accedendo, **registrare** tutti gli accessi e **monitorare** eventuali attività sospette.

Ambiti di protezione: **Data Loss / Insider Threat** (controllando gli accessi e le attività si minimizza la possibilità danneggiamento volontario o involontario dei sistemi e la sottrazione di dati)

VULNERABILITY ASSESSMENT PERIODICI SU TUTTO IL PERIMETRO

Con **Vulnerability Assessment** si intende quel processo finalizzato a **identificare e classificare i rischi e le vulnerabilità**, in termini di sicurezza, dei sistemi informativi aziendali. In pratica si tratta di un vero e proprio **scanning degli asset IT**, una fotografia dei sistemi informatici mirata a verificare quanto un'Azienda sia esposta e quali rischi corre nel caso in cui le protezioni di cui si è dotata dovessero venire bypassate in caso di cyber attacco.

Di seguito un elenco (non esaustivo) delle più diffuse vulnerabilità:

- porte di rete non necessarie lasciate aperte su server, router e/o firewall
- servizi di rete non sicuri contenenti vulnerabilità
- accessi ai sistemi non autorizzati o avvenuti senza autenticazione
- software obsoleti, spesso oggetto di attacco da parte di hacker
- sistemi informatici installati e lasciati con impostazioni di fabbrica

Eseguire test periodici sulle vulnerabilità di tutti i sistemi informatici è quindi estremamente importante per un'Azienda e può persino risultare fondamentale per la sopravvivenza del business: scoprire in anticipo i propri punti deboli permette infatti di adottare prontamente le opportune contromisure preventive.

Lo sviluppo e l'applicazione di una politica di sicurezza rigorosa, che include la valutazione della vulnerabilità, è fondamentale per mantenere la continuità operativa di un'azienda e ridurre al minimo la possibilità di Data Breach.

Gruppo San Donato

CAMPAGNE DI PHISHING PERIODICHE

Il **Phishing**, a differenza dello Spam, è un tipo di **truffa** effettuata normalmente da Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire **informazioni personali, dati finanziari o codici di accesso**, fingendosi un ente affidabile in una comunicazione digitale.

Questo fenomeno è da molti anni in costante aumento sia numerico che, soprattutto, qualitativo e quindi anche i migliori antispam presenti sul mercato, pur bloccando la quasi totalità delle email di phishing, a volte ne lasciano passare qualcuna (specialmente quelle scritte usando le tecniche più recenti e sofisticate). Per proteggersi, ogni Azienda deve inevitabilmente investire sul "fattore umano", allenando la capacità di ogni utente nel riconoscere un attacco Phishing nelle molte mail che si ricevono quotidianamente; solo così si può aumentare la resilienza e ridurre il livello di rischio dell'intera organizzazione.

Le Campagne di Phishing sono quindi simulazioni effettuate con periodicità «pseudocasuale» e sono solitamente suddivise in 3 fasi:

1) **Deception** - Vengono inviate ai dipendenti, senza preavviso, email ingannevoli con gradi di difficoltà differenziate e con un metodo di distribuzione che evita il fenomeno del "passaparola". Dopo la prima campagna, gli attacchi vengono personalizzati sulla base del profilo comportamentale di ogni individuo, attacchi dello stesso grado di difficoltà per chi è caduto nell'inganno, e di difficoltà crescente per chi non ha cliccato nella email.
2) **Report** – Viene prodotta reportistica comprendente metriche avanzate che consentono di avere una chiara lettura della situazione e di valutare l'analisi comportamentale come il click-rate, il rischio combinato (che tiene conto del livello di difficoltà degli attacchi), il livello di resilienza dell'organizzazione, ecc.
3) **Training** – A tutti coloro che cadono nell'inganno, viene effettuato un training, che li aiuterà a comprendere l'errore commesso e ad evitarlo in futuro.

Ambiti di protezione: **Awareness**

Gruppo San Donato

SISTEMA CLOUD ANTI DDOS

Un attacco DDoS (Distribuited Denial of Service) ha lo scopo di «sovraccaricare» un server, un servizio o un'infrastruttura informatica inviando un numero altissimo di richieste in un breve lasso di tempo in modo da saturarne le risorse impedendogli di rispondere al traffico legittimo.

Per fare un esempio, il più massiccio attacco DDoS registrato finora è avvenuto nel febbraio 2020, e ha avuto come obiettivo i server di Amazon Web Services (AWS). L'attacco ha generato, al suo apice, **traffico per 2,3 Terabit per secondo (Tbps)**, con l'invio di **1,1 miliardi di pacchetti di richieste**.

Qualsiasi sistema on-premise ha un proprio limite fisico di «resistenza» agli attacchi DDoS e quindi l'unico modo per proteggersi dagli attacchi più potenti è quello di dotarsi di soluzioni cloud le quali, potendo distribuire il traffico in ingresso su un numero elevato di apparati, sono in grado di bloccare quasi tutti i tipi di attacchi **analizzando in tempo reale e a grande velocità tutti i pacchetti di rete**, separando i pacchetti IP non legittimi dal resto e lasciando passare solo il traffico valido.

Grazie a questi sistemi, si mette in sicurezza la continuità operativa dei servizi esposti su internet (siti, portali, posta, ecc)

Ambiti di protezione: **Denial of Service (DoS)**.

Gruppo San Donato

MDM

Le piattaforme di Mobile Device Management (MDM) consentono di distribuire e gestire in modo sicuro qualsiasi software su qualunque dispositivo, integrando funzionalità di **controllo dell'accesso, gestione delle applicazioni e gestione degli endpoint multipiattaforma**, consentendo il controllo completo del dispositivo e dei suoi contenuti che, in caso ad esempio di furto o smarrimento, possono essere rimossi istantaneamente. Le soluzioni più evolute, abbinano alle funzionalità tipiche di enrollment o di "wipe" dei dati e «rintracciamento» dei dispositivi, **anche strumenti di controllo del dato che vi transita**, unitamente a protocolli di sicurezza automatizzati che con algoritmi di «analisi comportamentale» basati sul machine learning, possono intervenire nella segnalazione di anomalie, bloccare l'apparato o cancellarne i contenuti.

L'adozione della soluzione MDM garantisce la possibilità di gestire centralmente la sicurezza degli apparati aziendali mobili (Smartphone, Tablet e Notebook) o, in senso ancora più esteso, il controllo dei dati aziendali che transitano sui dispositivi mobili su cui si configurerà in modalità gestita e controllata, l'accesso ai dati aziendali come ad esempio la posta, i set di applicazioni consentite e la relativa configurazione operativa (ad esempio la configurazione delle app di messaggistica istantanea).

La soluzione prevede specifiche profilazioni dedicate alla protezione degli asset in uso ai VIP, ai quali è riservata una gestione in via preferenziale per l'immediata risposta ad esigenze o ad eventi specifici, consolidando ed irrobustendo le procedure già implementate a tutela (come ad esempio il wipe certificato con l'utilizzo della piattaforma Blancco ed il conseguente «vaulting» degli asset dismessi).

La soluzione proposta tiene in considerazione un modello di sottoscrizione «per utente» e non «per device». Per ogni utente possono essere configurati fino a 5 device con estensione della copertura della piattaforma anche ad asset non aziendali – BYOD (Bring Your Own Device)

Ambiti di protezione: **Malware, Web Based Attacks, Insider Threat, Awareness**

Gruppo San Donato

laboratorio SANITÀ 2030
14-15 GIUGNO 2023 LOMBARDIA
FIERA DI BERGAMO

SISTEMA EVOLUTO DI PROTEZIONE ENDPOINT CENTRALIZZATO (Total Breach Protection)

L'incremento del numero e delle tipologie di attacchi rende ad oggi necessario un **rafforzamento** della difesa degli endpoint (server e client) tramite l'introduzione di **Sistemi Evoluto di Protezione (xDR)** in sostituzione degli attuali antivirus ormai inefficaci di fronte agli attacchi più sofisticati. In GSD > 3000 server e 15.000 client.

I più completi tra i Sistemi xDR includono non solo funzionalità di Endpoint Protection Platform (EPP) ed Endpoint Detection and Response (EDR), ma anche tecnologie aggiuntive per coprire l'intero ambiente aziendale, inclusi gli host, la rete, i file e gli utenti. In particolare:

- **Network analytics** e **Inventory management** (discovery e catalogo automatico dei sistemi presenti in rete per identificare eventuali non autorizzati),
- **Data Lost Prevention** (individuazione e prevenzione dell'uso non autorizzato e della trasmissione di informazioni riservate),
- **Deception via Decoy Files, Folders, Servers, Services and Shares** (gli attaccanti, pensando di ottenere dati riservati, accedono ad "esche" fasulle messe in punti strategici dell'infrastruttura informatica; questa operazione scatena un alert immediato sulla console di controllo).

Ambiti di protezione: **Malware, Phishing, Data Breaches, Data Loss / Insider Threat**

Gruppo San Donato

FRAMEWORK CYBERSECURITY

Il **Framework CyberSecurity GSD** definisce le Policy, i Processi e le Procedure che tutte le Strutture del Gruppo devo adottare al fine di mantenere un alto livello di resilienza di fronte ai sempre più sofisticati attacchi informatici e sarà stilato sulla base del «Framework Nazionale per la Cybersecurity e la Data Protection» (https://www.cybersecurityframework.it/) il quale è suddiviso in cinque principali tematiche:

- **Identify (ID)**, ovvero la comprensione del contesto aziendale e degli asset critici per il business. Qui dentro si sviluppano controlli sull'asset management, sulla governance della cyber security, sulla gestione del rischio e dei dati, incluso il rischio filiera (Supply Chain Risk Management).
- **Protect (PR)**, tematica che racchiude misure volte alla protezione di processi di business, di asset aziendali ed informazioni. Tratta problematiche di controllo accessi, awareness, data security, tecnologie di protezione e la corretta manutenzione dei sistemi.
- **Detect (DE)**, comprende tutto ciò che è necessario all'identificazione di incidenti di sicurezza. Qui vengono trattate tematiche quali la gestione di anomalie ed eventi, il monitoraggio di sicurezza ed i processi di rilevamento.
- **Respond (RS)**, funzione dove si sviluppano le attività e gli interventi in caso di incidente di sicurezza informatica. Si va dalla pianificazione della risposta, alle analisi da condurre, alle mitigazioni, al contenimento della problematica, sino alle comunicazioni e le notifiche da emanare.
- **Recover (RE)**, funzione associata alle attività di ripristino di processi e servizi impattati da un incidente di sicurezza. I controlli in queste sezioni si articolano in tematiche quali il Recovery Planning, gli aspetti comunicativi ed i processi di miglioramento (Lesson Learned)

Gruppo San Donato

CORSI OBBLIGATORI DI FORMAZIONE SU CYBERSECURITY PER PERSONALE IT E DIPENDENTI

La sicurezza informatica non è solamente difesa dei software e degli asset aziendali, ma è, innanzitutto, prevenzione utilizzando i giusti strumenti ed **educando i dipendenti sui pericoli a cui sono sottoposti ogni giorno**.

I dipendenti infatti giocano un ruolo fondamentale quando si parla di mantenere la sicurezza all'interno dell'Azienda, poiché sono direttamente coinvolti nell'utilizzo di software, macchinari e piattaforme lavorative che interagiscono tra di loro. La ventesima edizione della EY Global Information Security Survey, intitolata "Cybersecurity regained: preparing to face cyber attacks", evidenzia infatti che i **dipendenti negligenti o inconsapevoli** sono la causa più probabile di un attacco, **anche più della criminalità organizzata e dei dipendenti malintenzionati**.

E' quindi necessario organizzare, con il coinvolgimento di HR, un piano di **formazione periodico con certificazione obbligatoria** (superamento test di fine corso) sulla CyberSecurity che coinvolga tutti i dipendenti di tutte le Strutture del Gruppo (sanitari, amministrativi, IT, ecc.).

I corsi dovranno essere personalizzati a seconda del «livello di rischio» di ciascun partecipante: più è alto il rischio (es. gli Utenti VIP che normalmente hanno accesso a dati estremamente riservati/sensibili) e più le tematiche affrontate durante il corso dovranno essere ampie ed approfondite.

Ambiti di protezione: Awareness

Gruppo San Donato

laboratorio SANITÀ 2030™
14-15 GIUGNO 2023 LOMBARDIA
FIERA DI BERGAMO

Creazione di un Team interno/esterno di SECURITY GOVERNANCE

Di seguito i principali task operativi:

1. Messa a terra dei **Progetti IT Security** (PAM, SIEM interno, XDR, WAF, Piattaforma di Identity ed Access Management, ecc.)
2. Definizione/aggiornamento delle procedure di **Incident Management**
3. Aggiornamento periodico dei **«casi d'uso» del SIEM** per ottimizzare le segnalazioni e massimizzarne l'efficacia
4. Analisi periodica delle **vulnerabilità di tutti i sistemi** informatici GSD (sia on premise che in cloud) e loro messa in sicurezza, con particolare attenzione ai servizi critici
5. Definizione/aggiornamento dei **KPI di sicurezza** (sia tecnologici che di processo)
6. Partecipazione ai **Progetti/Iniziative di Gruppo** a garanzia del rispetto dei requisiti di sicurezza «by design»
7. Stesura di policy di **codifica sicura per i fornitori applicativi** (es. raccomandazioni OWASP, utilizzo di algoritmi di crittografia non proprietari, ecc.)
8. Collaborazione con Operation e Sviluppo per la definizione e la messa in esercizio delle misure di sicurezza necessarie per i nuovi sistemi/network/applicazioni o per modifiche significative agli stessi (**Change Management**)
9. Verifica del **rispetto delle misure di sicurezza** necessarie per i nuovi sistemi/network/applicazioni (o per modifiche significative agli stessi) ed autorizzare o negare la messa in produzione.
10. Collaborazione con Operation per la definizione e implementazione di **Passive Asset Discovery Tool**
11. Collaborazione con Sviluppo per la definizione e implementazione di **Software Inventory Tools**
12. Partecipazione **«on demand» al CAB**

Gruppo San Donato

Creazione di un Team interno o esterno di SECURITY GOVERNANCE

12. Definizione/aggiornamento **«Forensic Readyness»** (definizione strumenti e modalità di acquisizione forense dei sistemi interessati prima che essi siano ripristinati)
13. Esecuzione **Incident Handling** sui sistemi di GSD (analisi dell'accaduto a valle di attacchi informatici)
14. Audit a campione sulla **sicurezza «outsurcer e terze parti»** per verificare che i Fornitori che operano utilizzando risorse di GSD siano in grado di garantire le misure di sicurezza a tutela degli asset e delle informazioni utilizzate, contemperando le esigenze di sicurezza con i livelli di servizio concordati in modo da garantire in ogni momento il rispetto delle misure di sicurezza di GSD.
15. Collaborazione con Responsabile della Formazione per la definizione dei temi da affrontare nei **corsi di aggiornamento** per dipendenti sulla CyberSecurity
16. Collaborazione con DPO per stesura/aggiornamento periodico del documento di **Risk Analysis**
17. Definizione **procedure per acquisizione e gestione apparati medicali** (definizione e implementazione di una procedura strutturata e vincolata da un workflow che non consenta installazione di apparati medicali senza il coinvolgimento preliminare della funzione IT Security)
18. **Partecipazione a corsi di formazione** periodici e certificazioni

Gruppo San Donato

Creazione di un Team (preferibilmente interno o servizio esterno con presidio locale) di INCIDENT RESPONSE

Di seguito i principali task operativi:

1. Monitoraggio costante dell'infrastruttura informatica di Gruppo, tramite le **console del SIEM / Antivirus / Antispam / ecc**.
2. Monitoraggi puntuali (es. **utenti VIP** e quelli più a rischio)
3. Monitoraggio dei media alla ricerca di eventuali **nuove vulnerabilità e nuove campagne di attacchi** (es. Polizia Postale, CISIRT, ecc.)
4. Monitoraggio costante del **Web** alla ricerca di informazioni riconducibili a GSD (credenziali, dati/informazioni riservate, ecc.)
5. Interventi tattici su apparati di protezione (es. firewall, WAF, antispam, antivirus, ecc.) per **bloccare eventuali attacchi in corso**, comunicando contestualmente l'evento sulla base dei processi di segnalazione/escalation definiti.
6. Collaborazione con Team di Incident Prevention per la **definizione delle remediation** di eventuali anomalie riscontrate e per eventuali miglioramenti delle segnalazioni e della sicurezza in generale
7. **Partecipazione a corsi di formazione** periodici e certificazioni

I componenti di questo team hanno buone conoscenze sui temi di networking e strumenti di gestione della sicurezza quali Firewall, IDS/IPS, Log Management, Antivirus, Antispam, xDR, ecc. e dovranno garantire, in reperibilità, la copertura delle 24 ore su 365 giorni/anno.

Gruppo San Donato

ESTENSIONE PERIMETRO

Per proteggere adeguatamente tutti i dati riservati, sensibili e personali esistenti all'interno di Gruppo San Donato, si adotta un estensione del perimetro coinvolgedo le aree ad oggi complementari a ICT ma ugualmente critiche e importanti, quali:

INGEGNERIA CLINICA

- Assessment finalizzato all'eliminazione di sistemi obsoleti/non sicuri
- Allineamento del processo autorizzativo per l'utilizzo e la messa in produzione di progetti e apparati medicali, che deve seguire lo standard di IT di Gruppo in termini di SDLC e Sicurezza.
- Ottenimento certificazioni relative alla sicurezza Informatica degli apparati medicali (cache con dati sensibili, esiti di esami, ecc)
- Sicurizzazione in termini di tracciamento degli apparati medicali mobili tramite asset tracking e allarmi perimetrali (furto)
- Estensione dei sistemi di videosorveglianza, con adozione di piattaforme centralizzate di controllo ed analisi comportamentale

RICERCA

- Assessment finalizzato a sostituire strumenti fai da te in favore di oggetti strutturati e sicuri
- Verifica e remediation infrastrutture, applicazioni in uso alla ricerca, senza concetto di sicurezza
- Allineamento del processo autorizzativo per l'utilizzo e la messa in produzione di progetti e strumenti in uso alla Ricerca allo standard di IT di Gruppo in termini di SDLC e sicurezza.

UNIVERSITA'

- Assessment finalizzato a sostituire strumenti fai da te in favore di oggetti strutturati e sicuri
- Verifica e remediation infrastrutture, applicazioni in uso, senza concetto di sicurezza
- Allineamento del processo autorizzativo per l'utilizzo e la messa in produzione di progetti e strumenti in uso all'Università allo standard di IT di Gruppo in termini di SDLC e sicurezza.

Gruppo San Donato

Delitti in materia di violazione del diritto d'autore (Art. 25-novies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009]

- Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, legge n.633/1941 comma 1 lett. a) bis)
- Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, legge n.633/1941 comma 3)
- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis legge n.633/1941 comma 1)
- Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis legge n.633/1941 comma 2)
- Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter legge n.633/1941)
- Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies legge n.633/1941)
- Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies legge n.633/1941).

Torna all'inizio