

S9

Traccia S9L1:

Durante la lezione teorica, abbiamo studiato le azioni preventive per ridurre la possibilità di attacchi provenienti dall'esterno.

Abbiamo visto che a livello di rete, possiamo attivare / configurare Firewall e regole per fare in modo che un determinato traffico, potenzialmente dannoso, venga bloccato.

La macchina Windows XP che abbiamo utilizzato ha **di default il Firewall disabilitato**.

L'esercizio di oggi è verificare in che modo l'attivazione del Firewall impatta il risultato di una scansione dei servizi dall'esterno. Per questo motivo:

1. Assicuratevi che il Firewall sia disattivato sulla macchina Windows XP
2. Effettuate una scansione con nmap sulla macchina target
3. Abilitare il Firewall sulla macchina Windows XP
4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch-sV.

Inoltre, definisci un'azienda cliente a cui fornirai questo servizio che rimarrà l'azienda di cui ti farai carico per tutta la settimana in termini di sicurezza informatica.

DanteNet Solutions S.r.l. è un'azienda specializzata nella fornitura di servizi di sicurezza informatica per imprese di medie e grandi dimensioni. L'azienda si occupa di proteggere le infrastrutture IT dei clienti attraverso una combinazione di consulenza, implementazione di soluzioni di sicurezza e monitoraggio continuo. I servizi offerti includono:

- Valutazione della Sicurezza di Rete: Analisi e verifica della sicurezza delle reti aziendali per identificare vulnerabilità e rischi potenziali.
- Implementazione di Firewall e Sistemi di Prevenzione delle Intrusioni (IPS): Configurazione e gestione di firewall e sistemi IPS per proteggere le reti da accessi non autorizzati e attacchi.
- Penetration Testing: Test di penetrazione per simulare attacchi reali e identificare punti deboli nel sistema di sicurezza.
- Monitoraggio e Risposta agli Incidenti: Monitoraggio continuo delle reti e risposta immediata agli incidenti di sicurezza per minimizzare i danni.
- Formazione sulla Sicurezza: Programmi di formazione per il personale aziendale per aumentare la consapevolezza e le competenze in materia di sicurezza informatica.

DanteNet Solutions S.r.l viene ingaggiata da SwissLab S.p.A. che è una società leader nel settore medico e delle biotecnologie, specializzata nelle analisi di laboratorio sul DNA e nelle tecnologie avanzate di ricerca medica con una solida reputazione a livello internazionale grazie alla sua eccellenza nella ricerca e nello sviluppo di soluzioni innovative per la diagnosi e il trattamento delle malattie genetiche.

SwissLab S.p.A. rappresenta una realtà all'avanguardia nel settore medico e biotecnologico, con un forte impegno verso l'innovazione e la qualità.

L'azienda offre servizi cruciali per la diagnosi e il trattamento delle malattie genetiche, supportando la comunità medica e scientifica nella diagnosi e nel trattamento dei pazienti, oltre che collaborare con diverse università in tutto il mondo.

SwissLab è consapevole della necessità di proteggere le informazioni sensibili, inclusi i dati dei pazienti, i dettagli sui prodotti medici e le informazioni proprietarie.

Per garantire la sicurezza delle proprie reti e sistemi, il cliente desidera:

- Valutare l'efficacia dei firewall esistenti su diverse versioni di sistemi operativi, inclusi quelli legacy come Windows XP, ancora in uso per alcune apparecchiature mediche.
- Identificare eventuali vulnerabilità che potrebbero essere sfruttate da attori malevoli.
- Ricevere raccomandazioni per migliorare la configurazione del firewall e altre misure di sicurezza.

NB: il preventivo che segue include soltanto i servizi richiesti nella traccia dell'esercizio di oggi e verrà implementato nel corso della settimana nel caso di servizi aggiuntivi dati nei prossimi esercizi.

Preventivo #1022

DanteNet Solution S.r.l
Via xxxx Milano, Italia
P.IVA: xxxxxxxxxxxxxxxxx

Cliente:

SwissLab S.p.A.
Via xxxxxx, Mendrisio, Svizzera
P.IVA xxxxxxxxxxxxxxxxx

Preventivo valido fino al 30.06.2024

Attività	Ore Stimate	Tariffa Oraria (€)	Costo Totale (€)
Valutazione Iniziale	5	100	500
Disabilitazione e Abilitazione del Firewall	4	100	400
Esecuzione delle Scansioni con Nmap	16	100	1.600
Redazione del Report	10	100	1.000
Presentazione e Discussione del Report	5	100	500
Totale	40		4.000

Termini e condizioni

- Il pagamento sarà effettuato al completamento di ciascuna fase del progetto, secondo le ore effettivamente lavorate.
- Eventuali costi aggiuntivi per materiali o risorse esterne non inclusi nel preventivo saranno discussi e approvati con il cliente prima di essere sostenuti.
- Le modifiche al progetto originale che richiedono ore di lavoro aggiuntive saranno fatturate separatamente.

Accettazione del Preventivo

Firma del Cliente: _____

Data: _____

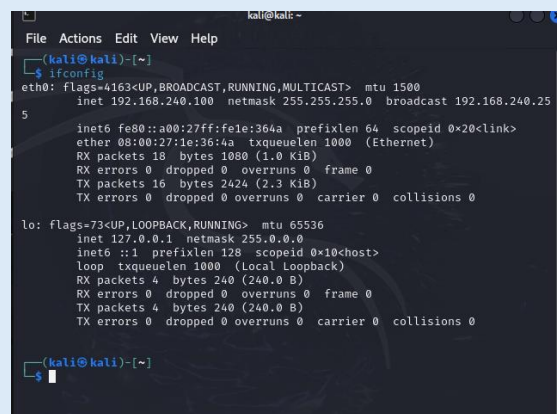
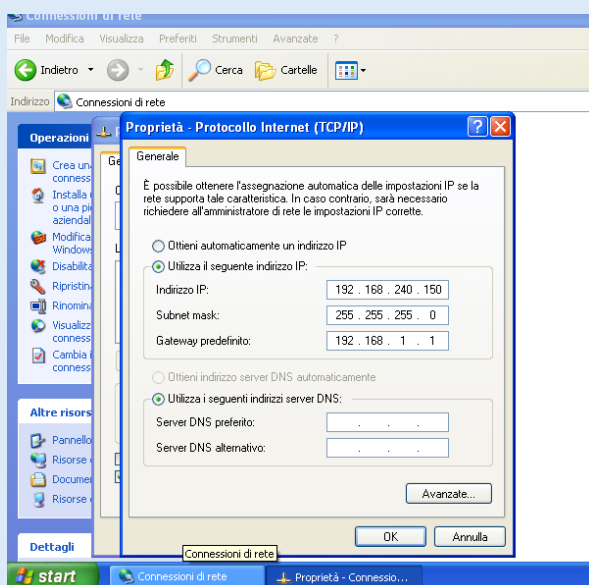
L'obiettivo dell'esercizio di oggi è quello di verificare come l'attivazione del firewall su una macchina Windows XP impatti i risultati di una scansione dei servizi effettuata dall'esterno utilizzando Nmap.

Come primo passaggio per lo svolgimento di questo esercizio, ho assegnato gli indirizzi IP richiesti alle due macchine.

Avremo quindi come da immagine

Windows XP con indirizzo IP: 192.168.240.150

Kali con indirizzo IP: 192.168.240.100.



Procedo quindi a verificare che il firewall di Windows XP sia disabilitato



Eseguo quindi la prima scansione nmap utilizzando il comando

```
nmap -sV 192.168.240.150
```

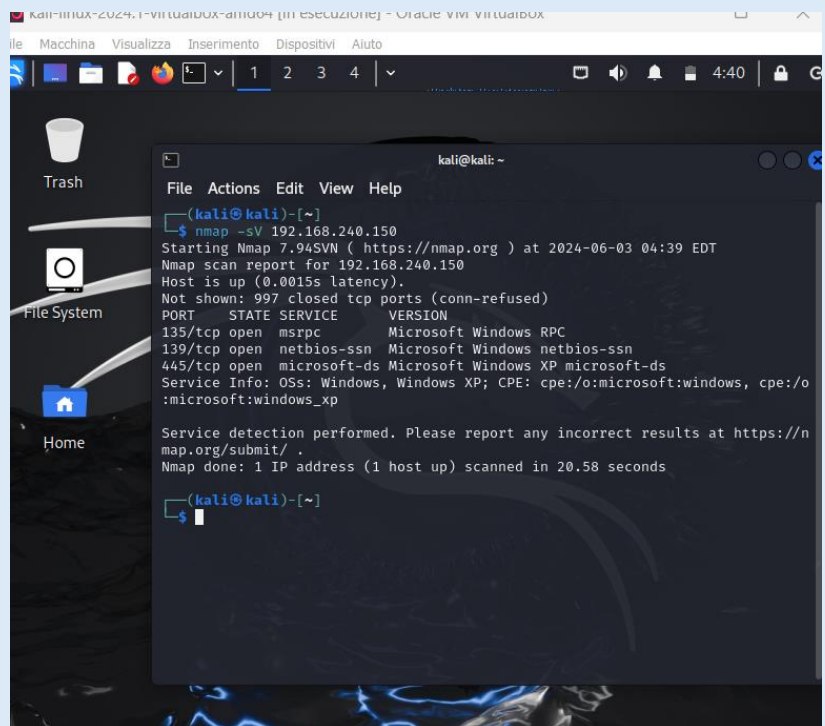
da Kali Linux per effettuare una service detection.

La scansione con il firewall disattivato ha rilevato 3 servizi in ascolto sulle seguenti porte TCP:

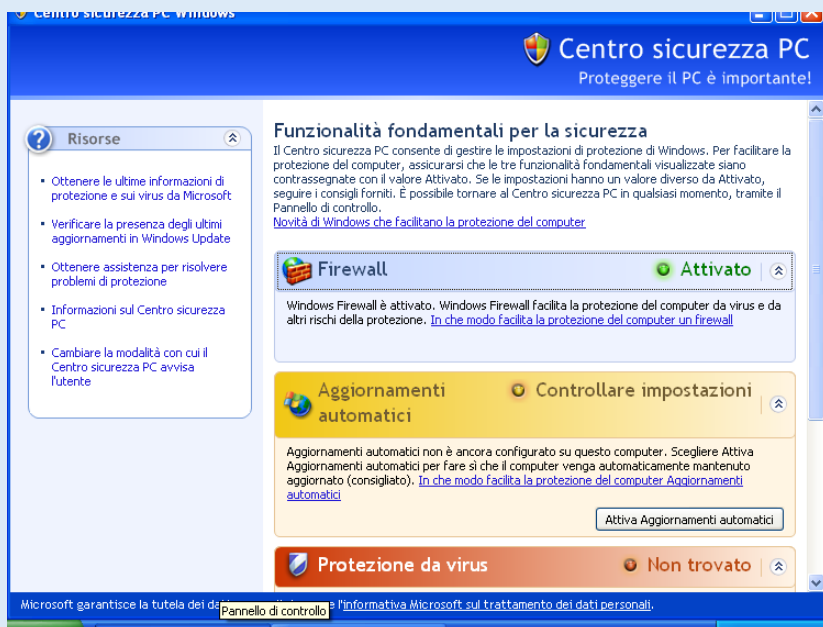
Porta 135: servizio Microsoft RPC

Porta 139: servizio NetBIOS-SSN

Porta 445: servizio Microsoft-DS



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nmap -sV 192.168.240.150  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 04:39 EDT  
Nmap scan report for 192.168.240.150  
Host is up (0.0015s latency).  
Not shown: 997 closed tcp ports (conn-refused)  
PORT      STATE SERVICE      VERSION  
135/tcp    open  msrpc        Microsoft Windows RPC  
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn  
445/tcp    open  microsoft-ds  Microsoft Windows XP microsoft-ds  
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 20.58 seconds  
  
(kali@kali)-[~]  
$
```



Tornando al pannello di controllo su Windows XP, dal centro sicurezza attivo il firewall

Eseguo nuovamente la scansione con Nmap utilizzando il comando

```
nmap -sV 192.168.240.150
```

da Kali Linux.

La scansione ha riportato che la macchina o non è accesa, oppure sta bloccando l'host discovery di Nmap.

```
(kali@kali)-[~]
$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 04:41 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try
-Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.14 seconds

(kali@kali)-[~]
$
```

Utilizzo quindi il comando

```
nmap -sV -Pn 192.168.240.150
```

per saltare il ping e passare direttamente alla service discovery.

La scansione indica che tutte le porte sembrano filtrate e non hanno risposto alle richieste dello scanner.

```
(kali@kali)-[~]
$ nmap -sV 192.168.240.150 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 04:43 EDT
Nmap scan report for 192.168.240.150
Host is up.
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 215.29 seconds

(kali@kali)-[~]
$
```

Conclusioni

L'attivazione del firewall su una macchina Windows XP ha un impatto significativo sui risultati di una scansione dei servizi effettuata con Nmap.

Con il firewall disattivato, Nmap è stato in grado di rilevare tre servizi attivi sulle porte TCP 135, 139 e 445. Tuttavia, una volta attivato il firewall, la macchina ha bloccato l'host discovery di Nmap, rendendo impossibile la rilevazione dei servizi.

Utilizzando l'opzione **-Pn**, che forza Nmap a saltare il ping e procedere direttamente alla scoperta dei servizi, tutte le porte sono risultate filtrate. Questo indica che il firewall sta bloccando attivamente il traffico in ingresso, non rispondendo alle richieste di Nmap.

Questi risultati dimostrano l'efficacia del firewall di Windows XP nel bloccare tentativi di scansione esterna, aumentando significativamente la sicurezza della macchina contro possibili attacchi. L'attivazione del firewall è quindi una misura preventiva cruciale per proteggere i sistemi da traffico potenzialmente dannoso.

Traccia S9L2:

Esercizio Business continuity & disaster recovery Durante la lezione teorica, abbiamo affrontato gli argomenti riguardanti la business continuity e disaster recovery.

Nell'esempio pratico di oggi, ipotizziamo di essere stati assunti per valutare quantitativamente l'impatto di un determinato disastro su un asset di una compagnia.

Con il supporto dei dati presenti nelle tabelle che seguono, calcolare la perdita annuale che subirebbe la compagnia nel caso di:

- Inondazione sull'asset «edificio secondario»
- Terremoto sull'asset «datacenter»
- Incendio sull'asset «edificio primario»
- Incendio sull'asset «edificio secondario»
- Inondazione sull'asset «edificio primario»

Dati:

ASSET	VALORE
Edificio primario	350.000€
Edificio secondario	150.000€
Datacenter	100.000€

EVENTO	ARO
Terremoto	1 volta ogni 30 anni
Incendio	1 volta ogni 20 anni
Inondazione	1 volta ogni 50 anni

EXPOSURE FACTOR	Terremoto	Incendio	Inondazione
Edificio primario	80%	60%	55%
Edificio secondario	80%	50%	40%
Datacenter	95%	60%	35%

Per valutare quantitativamente l'impatto di un disastro su un asset di una compagnia e calcolare la perdita annuale attesa, utilizziamo il concetto di Annual Loss Expectancy (ALE).

L'ALE viene calcolata come il prodotto tra la probabilità annuale dell'evento e la perdita attesa per evento (Single Loss Expectancy, SLE).

La formula per la SLE è:

$SLE = \text{valore dell'asset} * \text{exposure factor (EF)}$

La formula per la ALE è:

$ALE = SLE * ARO$ (Annualized Rate of Occurrence)

I dati forniti sono:

- Edificio primario: valore 350.000€
- Edificio secondario: valore 150.000€
- Datacenter: valore 100.000€

Eventi e frequenze:

- Terremoto: $ARO = 1/30$
- Incendio: $ARO = 1/20$
- Inondazione: $ARO = 1/50$

Exposure factor (EF) per ogni asset e tipo di evento:

- Edificio primario:
 - Terremoto: 80%
 - Incendio: 60%
 - Inondazione: 55%
- Edificio secondario:
 - Terremoto: 80%
 - Incendio: 50%
 - Inondazione: 40%
- Datacenter:
 - Terremoto: 95%
 - Incendio: 60%
 - Inondazione: 35%

Calcoli:

Ricordando che: $1/50 = 0,02$; $1/20 = 0,05$; $1/30 = 0,0333$

1. Inondazione sull'asset "edificio secondario"

- $SLE = 150.000 \text{ €} * 40\% = 60.000 \text{ €}$
- $ARO = 1/50$
- $ALE = 60.000 \text{ €} * (1/50) = 1.200 \text{ €}$

2. Terremoto sull'asset "datacenter"

- $SLE = 100.000 \text{ €} * 95\% = 95.000\text{€}$
- $ARO = 1/30$
- $ALE = 95.000 \text{ €} * (1/30) = 3.163 \text{ €}$

3. Incendio sull'asset "edificio primario"

- $SLE = 350.000 \text{ €} * 60\% = 210.000 \text{ €}$
- $ARO = 1/20$
- $ALE = 210.000 \text{ €} * (1/20) = 10.500\text{€}$

4. Incendio sull'asset "edificio secondario"

- $SLE = 150.000\text{€} * 50\% = 75.000 \text{ €}$
- $ARO = 1/20$
- $ALE = 75.000\text{€} * (1/20) = 3.750 \text{ €}$

5. Inondazione sull'asset "edificio primario"

- $SLE = 350.000 \text{ €} * 55\% = 192.500 \text{ €}$
- $ARO = 1/50$
- $ALE = 192.500 \text{ €} * (1/50) = 3.850 \text{ €}$

6. Terremoto sull'asset "edificio primario"

- $SLE = 350.000 \text{ €} * 80\% = 280.000 \text{ €}$
- $ARO = 1/30$
- $ALE = 280.000 \text{ €} * (1/30) = 9.324 \text{ €}$

Preventivo #1023

DanteNet Solution S.r.l
Via xxxx Milano, Italia
P.IVA: xxxxxxxxxxxxxxxxxxxx

Cliente:

SwissLab S.p.A.
Via xxxxxx, Mendrisio, Svizzera
P.IVA xxxxxxxxxxxxxxxxxxxx

Preventivo valido fino al 30.06.2024

Attività	Ore Stimate	Tariffa Oraria (€)	Costo Totale (€)
Analisi preliminare e Raccolta Dati	20	100	2.000
Sviluppo del Piano di Continuità Operativa	40	100	4.000
Sviluppo del Piano di Disaster Recovery	30	100	3.000
Formazione e Comunicazione	15	100	1.500
Revisione del Piano	15	100	1.500
Documentazione e Consegna del Piano	10	100	1.500
Totale	130		13.000

Termini e condizioni

- Il pagamento sarà effettuato al completamento di ciascuna fase del progetto, secondo le ore effettivamente lavorate.
- Eventuali costi aggiuntivi per materiali o risorse esterne non inclusi nel preventivo saranno discussi e approvati con il cliente prima di essere sostenuti.
- Le modifiche al progetto originale che richiedono ore di lavoro aggiuntive saranno fatturate separatamente.

Accettazione del Preventivo

Firma del Cliente: _____

Data: _____

Business Continuity and Disaster Recovery Plan (BCDRP)

Compagnia: SwissLab S.p.A.

Data: 4 Giugno 2024

Introduzione

Questo piano descrive le procedure per garantire la continuità operativa e il ripristino delle attività aziendali in caso di disastro che colpisca gli asset critici della compagnia SwissLab S.p.A. Il piano è stato sviluppato per mitigare i rischi associati a inondazioni, terremoti e incendi.

Obiettivi

- Garantire la continuità delle operazioni critiche di ricerca e sviluppo.
- Proteggere i campioni biologici, i dati clinici e le attrezzature sensibili.
- Ridurre al minimo l'impatto finanziario di disastri su asset chiave.
- Stabilire procedure di risposta e ripristino efficienti per la sicurezza dei pazienti e dei dati.

Asset Critici e Valutazione dei Rischi

Asset	Valore (€)	Tipo di Evento	Probabilità (ARO)	Exposure Factor (EF)	Single Loss Expectancy (SLE) (€)	Annual Loss Expectancy (ALE) (€)
Edificio primario	350.000	Inondazione	1/50	55%	192.500	3.850
Edificio primario	350.000	Terremoto	1/30	80%	280.000	9.324
Edificio primario	350.000	Incendio	1/20	60%	210.000	10.500
Edificio secondario	150.000	Inondazione	1/50	40%	60.000	1.200
Edificio secondario	150.000	Incendio	1/20	50%	75.000	3.750
Datacenter	100.000	Terremoto	1/30	95%	95.000	3.163

Strategie di Mitigazione

Inondazione:

- Installazione di sistemi di drenaggio e pompe per prevenire accumuli d'acqua.
- Elevazione di laboratori critici e magazzini di campioni biologici al di sopra del livello di inondazione previsto.
- Utilizzo di contenitori ermetici per la conservazione dei campioni biologici.
- Implementazione di barriere contro le inondazioni intorno all'edificio.
- Monitoraggio e allerta precoce per eventi meteorologici estremi.

Terremoto:

- Rafforzamento strutturale dell'edificio per resistere a scosse sismiche.
- Sistemi di scaffalature antisismiche per le attrezzature e i reagenti chimici.
- Implementazione di sistemi di protezione delle apparecchiature IT contro i terremoti.
- Backup regolari dei dati clinici e di ricerca in siti remoti e cloud.
- Sistemi di ridondanza per garantire la disponibilità continua dei dati.

Incendio:

- Installazione di sistemi antincendio avanzati, inclusi sprinkler e rilevatori di fumo.
- Formazione del personale in tecniche di evacuazione e uso di estintori.
- Protocollo di sicurezza per il trattamento di materiali infiammabili e reattivi.
- Sistemi di rilevazione e soppressione del fuoco.
- Regolare manutenzione e ispezione degli impianti elettrici e delle attrezzature.
- Procedure di emergenza per la manipolazione di sostanze pericolose.

Rischi di Cybersecurity in Caso di Disastri Naturali

- **Perdita di Dati e Sistemi**

Danni fisici ai server, ai data center e ai dispositivi di archiviazione che possono portare alla perdita di dati critici.

Perdita permanente di dati importanti, interruzione delle operazioni aziendali, compromissione della ricerca e sviluppo.

- **Accesso Fisico Non Autorizzato**

Durante un disastro, le misure di sicurezza fisica possono essere compromesse, permettendo l'accesso non autorizzato ai sistemi e ai dati.

Furto di dati sensibili, alterazione o distruzione di informazioni, esposizione a minacce interne ed esterne.

- **Interruzione delle Comunicazioni e Controlli di Sicurezza**

Interruzioni delle reti di comunicazione e dei sistemi di controllo di sicurezza possono lasciare i sistemi vulnerabili ad attacchi.

Inabilità a monitorare e rispondere a minacce in tempo reale, aumentando il rischio di attacchi informatici durante il disastro.

- **Corruzione dei Dati**

Danneggiamento fisico o corruzione dei dati a causa di disastri naturali può compromettere l'integrità delle informazioni.

Dati danneggiati o alterati possono portare a decisioni errate, compromissione della qualità della ricerca e perdita di fiducia da parte dei clienti e dei partner.

Strategie di Mitigazione legate alla Cybersecurity

- **Backup e Ripristino dei Dati**

Implementazione di backup regolari e sicuri, archiviati in sedi diverse e nel cloud, per garantire la disponibilità dei dati anche in caso di disastri fisici.

Sviluppo di procedure dettagliate per il ripristino dei dati e dei sistemi, con test regolari per assicurare l'efficacia del processo.

- **Sicurezza Fisica e Accesso Controllato**

Rafforzamento delle misure di sicurezza fisica nei data center e nei laboratori, inclusi controlli di accesso rigorosi, videosorveglianza e sistemi di allarme.

Implementazione di sistemi di controllo degli accessi fisici e logici, con autenticazione a più fattori per limitare l'accesso ai dati critici.

- **Ridondanza e Alta Disponibilità**

Progettazione di infrastrutture IT ridondanti per garantire la continuità operativa anche in caso di guasti fisici. Questo include server di backup, data center secondari.

- **Piani di Continuità Operativa e Recupero di Emergenza**

Sviluppo di piani dettagliati per mantenere operazioni critiche durante e dopo un disastro, includendo l'allocazione di risorse, la comunicazione di crisi e la gestione del personale.

Documentazione di piani di disaster recovery specifici per la ripresa dei sistemi IT, con procedure dettagliate e responsabili assegnati.

- **Formazione e Sensibilizzazione del Personale**

Educazione continua del personale sulle procedure di emergenza, la sicurezza dei dati e le pratiche di cybersecurity durante i disastri.

Conduzione di esercitazioni regolari per simulare scenari di disastro e verificare l'efficacia dei piani di continuità operativa e disaster recovery.

- **Monitoraggio e Risposta agli Incidenti**

Costituzione di un team dedicato di risposta agli incidenti con protocolli chiari per la gestione delle emergenze di cybersecurity.

Piano di Risposta e Ripristino

- **Attivazione del Team di Risposta ai Disastri:**

Composto da rappresentanti IT, sicurezza, gestione edifici, direzione e responsabili di laboratorio.

Coordinamento con le autorità locali, i servizi di emergenza e le agenzie di regolamentazione.

- **Valutazione del Danno:**

Ispezione immediata degli asset colpiti per determinare l'entità del danno.

Documentazione dei danni per la successiva richiesta di indennizzo assicurativo.

Messa in sicurezza dei campioni biologici e dei dati sensibili.

- **Ripristino Temporaneo:**

Trasferimento delle operazioni critiche di laboratorio in strutture alternative, se necessario.

Attivazione di backup dati e sistemi IT in siti remoti.

Controllo della qualità e dell'integrità dei campioni biologici.

- **Ripristino Completo:**

Riparazione e ristrutturazione degli asset danneggiati.

Verifica e test dei sistemi ripristinati prima del ritorno alle operazioni normali.

Validazione della qualità dei processi e dei prodotti di laboratorio.

Comunicazione

Interna:

- Aggiornamenti regolari al personale sull'avanzamento del ripristino.
- Canali di comunicazione di emergenza (e-mail, messaggi, bacheche aziendali).

Esterna:

- Comunicazione con clienti, fornitori, partner di ricerca e altre parti interessate.
- Utilizzo di comunicati stampa e aggiornamenti sui social media per informare il pubblico e le agenzie di regolamentazione.
- Comunicazione con le autorità sanitarie e regolatorie in caso di impatti sui dati clinici o sulla ricerca.

Formazione e Test

- Programmi di formazione regolari per il personale su procedure di emergenza e sicurezza.
- Addestramento specifico per la manipolazione sicura di campioni biologici e reagenti pericolosi.
- Simulazioni di disastro e prove di evacuazione per verificare l'efficacia del piano.
- Revisione e aggiornamento del piano sulla base dei risultati dei test e dei feedback ricevuti.
- Valutazioni periodiche della conformità alle normative di sicurezza e di qualità.

Manutenzione del Piano

Il Business Continuity and Disaster Recovery Plan sarà riesaminato e aggiornato annualmente o in seguito a modifiche significative nelle operazioni aziendali, nell'infrastruttura o nel profilo di rischio. La revisione includerà l'analisi dei cambiamenti nelle normative del settore medico e biotecnologico.