

CYBER SECURITY

Lezione 04 – Gestione del Rischio

OBIETTIVO



Conoscere i principali elementi coinvolti nella valutazione del rischio:

- **beni** da difendere;
- **obiettivi** di sicurezza;
- **minacce** alla sicurezza;
- **vulnerabilità** dei sistemi informatici;
- **impatto** causato dall'attuazione delle minacce.

OBIETTIVO



Conoscere i principali elementi coinvolti nella valutazione del rischio:

- **beni da difendere;**
- obiettivi di sicurezza;
- minacce alla sicurezza;
- vulnerabilità dei sistemi informatici;
- **impatto** causato dall'attuazione delle minacce.

BENI



- *Un bene è qualsiasi cosa, materiale o immateriale, che abbia un valore e debba quindi essere protetta.*



BENI



Nel campo della sicurezza delle informazioni, tra i beni di un'azienda ci sono le risorse informatiche, il personale (utenti, amministratori, addetti alla manutenzione), le informazioni, la documentazione e l'immagine aziendale.

Per un individuo, i beni comprendono non solo risorse informatiche, informazioni e mezzi di comunicazione, ma anche le informazioni personali e la privacy.

BENI => DEFACING



- l'alterazione di un sito web per rovinare l'immagine del proprietario
- colpisce sia le informazioni sia l'immagine dell'azienda o persona titolare



BENI => PRIVACY



minacciata da più parti:

- aziende che non **proteggono** adeguatamente le informazioni in loro possesso,
- applicazioni che **trasmettono** via Internet dati personali,
- software maligno che **spia** le abitudini degli utenti (acquisti, navigazione Internet etc.) o che **altera** la navigazione Internet a scopo di truffa o furto di informazioni.



BENI



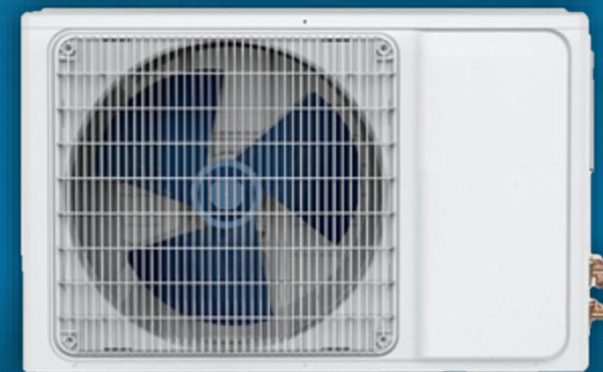
- beni **primari**, quelli che hanno valore effettivo;
- beni **secondari**, che servono per proteggere i beni primari.



BENI SECONDARI



- attrezzature che permettono all'hardware di funzionare con continuità e sicurezza
- costo ampiamente inferiore rispetto al rimedio a situazioni non previste.



OBIETTIVO



Conoscere i principali elementi coinvolti nella valutazione del rischio:

- **beni** da difendere;
- **obiettivi di sicurezza;**
- **minacce** alla sicurezza;
- **vulnerabilità** dei sistemi informatici;
- **impatto** causato dall'attuazione delle minacce.

OBIETTIVI DI SICUREZZA



grado di protezione che si intende predisporre per i beni, in termini di

- **disponibilità,**
- **integrità e**
- **riservatezza.**



OBIETTIVI DI SICUREZZA



- **CLASSIFICARE** beni in categorie e
- **CREARE** una mappa di ciò che è importante e da proteggere

Bene	Riservatezza	Disponibilita'	Integrita'
Password	X		
Dati Bancari	X	X	X
Info su Sito Web		X	X
...			

OBIETTIVO



Conoscere i principali elementi coinvolti nella valutazione del rischio:

- **beni** da difendere;
- obiettivi di sicurezza;
- **minacce alla sicurezza;**
- **vulnerabilità** dei sistemi informatici;
- **impatto** causato dall'attuazione delle minacce.

MINACCIA



Una minaccia è un'azione

- *potenziale,*
- *accidentale o*
- *deliberata,*

*che può portare alla
violazione di uno o più
obiettivi di sicurezza
posta in essere da un
AGENTE*



origine:

- **naturale,**
- **ambientale o**
- **umana**

MINACCE: ESEMPI



Minaccia	D	A	E
Terremoto			X
Inondazione		X	X
Uragano			X
Fulmine			X
Bombardamento	X	X	
Incendio	X	X	
Uso di Armi	X	X	
Vandalismo	X		
Furto	X		
Blackout		X	
Infiltrazioni in rete	X		

Minaccia	D	A	E
Linea El. Instabile		X	X
Guasto Clima		X	
Temperatura ↑↓	X	X	
Umidità' ↑	X	X	
Polvere	X	X	
EMP	X	X	
Guasti HW		X	
Uso improprio		X	X
Errori SW	X	X	
Uso non autorizzato supporti memoria		X	

Minaccia	D	A	E
Deterioramento HW			X
Errori Utenti	X	X	
Errori Manutenzione	X	X	
Accesso illegal NW	X		
Uso illegal pwd e sw	X		
SW dannoso	X	X	
Uso SW illegal	X		
Interruzione internet		X	
Errori RTx			X
Traffico eccessivo	X	X	
Intercettazioni		X	

OBIETTIVO



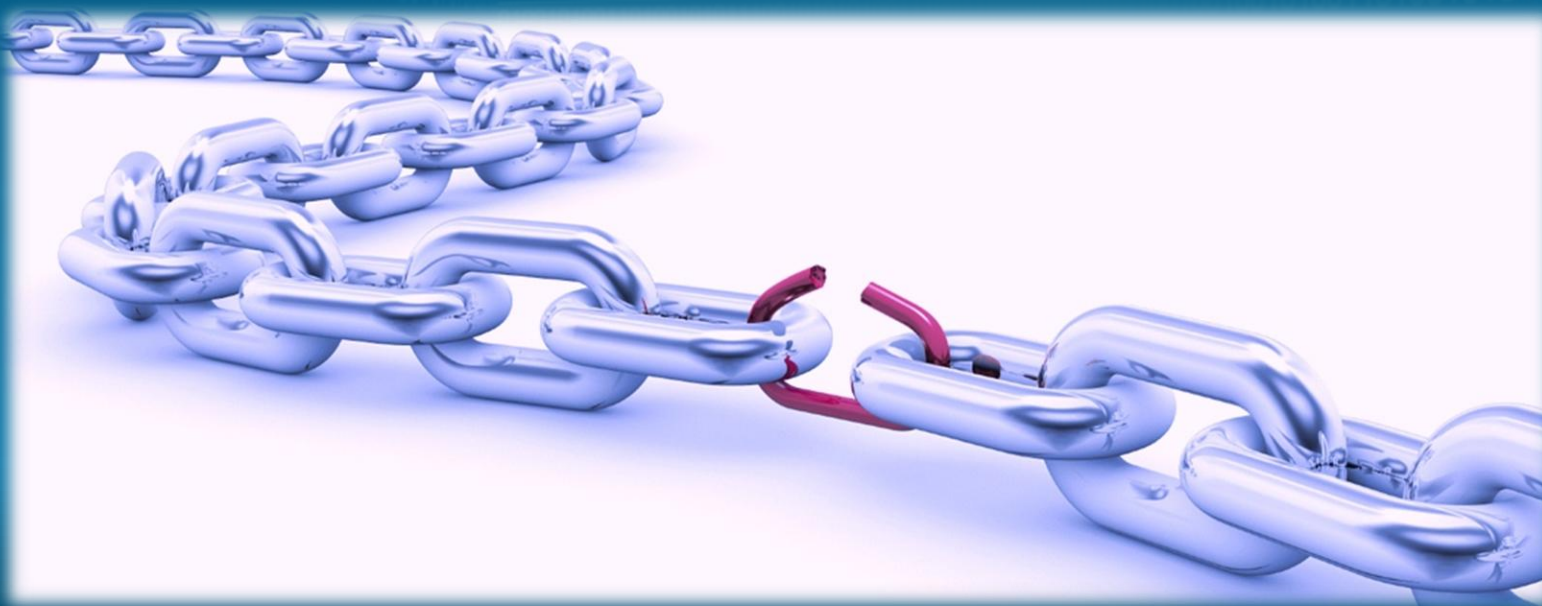
Conoscere i principali elementi coinvolti nella valutazione del rischio:

- **beni** da difendere;
- **obiettivi** di sicurezza;
- **minacce** alla sicurezza;
- **vulnerabilità dei sistemi informatici;**
- **impatto** causato dall'attuazione delle minacce.

VULNERABILITA'



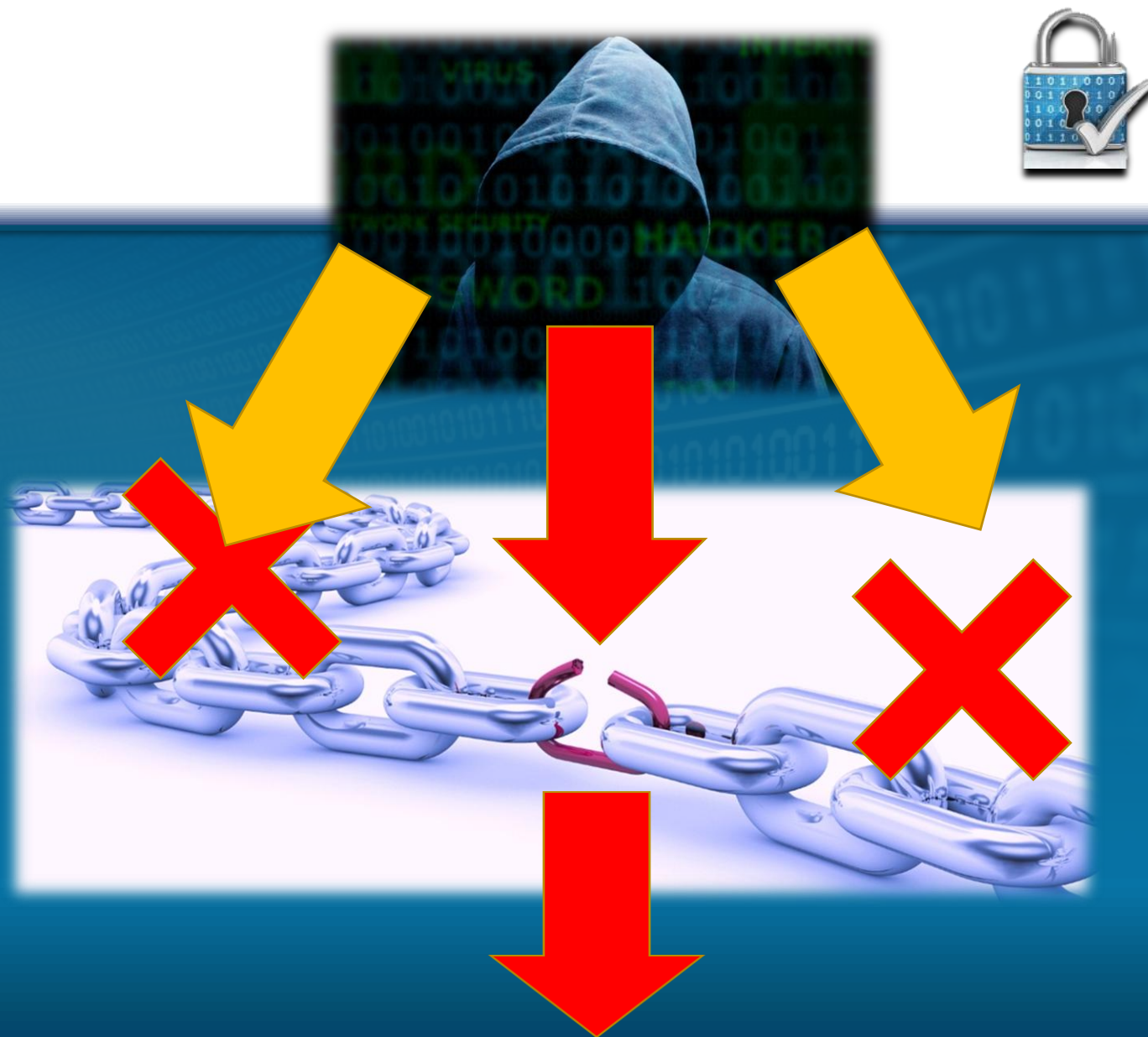
è un **punto debole** del sistema informatico (hardware, software e procedure) che, **se colpito o sfruttato** da una minaccia, porta alla violazione di qualche obiettivo di sicurezza.



è un aspetto
intrinseco
del sistema
informatico ed
esiste
indipendentemente
da fattori esterni

VULNERABILITA'

- Una vulnerabilità, di per sé, non causa automaticamente una perdita di sicurezza;
- è la **combinazione** tra vulnerabilità e minaccia che determina la probabilità che vengano violati gli obiettivi di sicurezza.



VULNERABILITA': ESEMPI



▪ Infrastrutturali

- NO protezione fisica
- NO ctrl accessi
- Linea elettrica instabile
- Possibilit  allagamento

▪ Software

- Apps complesse
- NO Autenticazioni
- NO Logging
- Errori SW noti
- NO PWD protette

▪ HW e impianti

- NO backup
- Influssi da var 220v
- Influssi da t  C
- Influssi EMP
- Poca manutenzione

▪ Comunicazioni

- NO protezione
- PWD in chiaro
- WiFi non cifrato
- Dial-Up
- NW Free Access

▪ Documentazione

- NO protezione locali
- NO controlli su eliminazione
- NO controlli su duplicazione

▪ Personale

- Nro Insufficiente
- NO controllo
- NO addestramento
- NO monitoraggio

OBIETTIVO



Conoscere i principali elementi coinvolti nella valutazione del rischio:

- **beni** da difendere;
- obiettivi di sicurezza;
- **minacce** alla sicurezza;
- **vulnerabilità** dei sistemi informatici;
- **impatto causato dall'attuazione delle minacce.**

IMPATTO



*è la conseguenza
dell'attuazione di una
minaccia.*

*Esso dipende dal valore del
bene colpito e dagli
obiettivi di sicurezza violati.*

