VALUTAZIONE E MITIGAZIONE DEL RISCHIO DI SICUREZZA CYBER

Artsiom Yautsiukhin

OUTLINE

- Come misurare la sicurezza cyber?
- Valutazione del rischio e termini relativi
- Valutazione del rischio cyber
  - Identificazione del rischio
    - Cyber assets
    - Tipiche minacce cyber
    - Controlli di sicurezza cyber
    - Strumenti e metodi
  - Analisi e ponderazione del rischio
- Trattamento del rischio
- Conclusione

3

COME MISURARE LA SICUREZZA CYBER?

COME MISURARE LA SICUREZZA CYBER?

"If you can't measure it, you can't improve it"
Lord Kelvin

- Obiettivo:
  - Prendere una decisione razionale per migliorare la tua sicurezza cyber.

- I problemi:
  - La decisione deve essere presa per **l'intero** sistema di sicurezza cyber;
  - Sicurezza cyber se molto **eterogenea** (include gestione, politiche, soluzioni tecniche, molteplici piccole opzioni per soluzioni tecnologiche, aspetti fisici e sociali, ecc.)
  - La decisione spetta ai **dirigenti**, non ai tecnici;
  - Le soluzioni di sicurezza (opzioni) sono **costose** e il budget per la sicurezza cyber è **limitato**;
  - Come prendere la decisione **razionalmente**? Quali misure/metriche utilizzare?
  - Anche sistemi IT simili sono **diversi**
  - Il contesto della sicurezza cyber **sta cambiando**

UN APPROCCIO: CONFORMITÀ

- Conformità in poche parole:
  - Un elenco di controlli di sicurezza da implementare viene fornito da qualcuno; ad esempio, da
    - Un dirigente superiore (per le imprese grandi)
    - Un regolatore (ad esempio, per le infrastrutture critiche)
    - Alcuni "standard"
  - È necessario implementare questi controlli
    - Può essere visto come una lista di controllo: un elenco di controlli che devono essere "spuntati".

- Pro:
  - Semplice
  - Poca responsabilità
  - Può essere utilizzato per ottenere un certificato (un processo molto più complesso)

- Contro:
  - La necessità di fidarsi della fonte che ha generato la lista di controlli
  - I controlli potrebbero non esserti utili
  - Facile da esagerare (spendi troppo)
  - Come definire un elenco di controlli?

LA SICUREZZA CYBER NON È SOLO UN PROBLEMA TECNICO!

CYBERSECURITY VENTURES

ABOUT RESEARCH LISTS VIDEOS EVENTS JO

Last year, Cybersecurity Ventures predicted that cybercrime will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015. This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, and will be more profitable than the global trade of all major illegal drugs combined.

Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019

Climate change a growing concern for global re/insurers: PwC

8th November 2021 - Author: Luke Gallin

The PwC Insurance Banana Skins 2021 survey shows that cybercrime is ranked as the number one risk by carriers globally, while climate change tops the list for reinsurers amid a rise in natural catastrophe events.

The latest global edition of the biennial survey includes responses from more than 600 industry leaders and executives in 47 territories, and shows that climate change has become a top concern for life, non-life, reinsurance and composite insurers.

Top 10 op risks 2020

	2020	2019	Change
IT disruption	1	2	↑
Data compromise	2	1	↓
Theft and fraud	3	5	↑
Outsourcing and third-party risk	4	6	↑
Resilience risk	5	–	
Organisational change	6	4	↓
Conduct risk	7	10	↑
Regulatory risk	8	7	↓
Talent risk	9	–	
Geopolitical risk	10	–	

ALTERNATIVA: VALUTAZIONE DEL RISCHIO

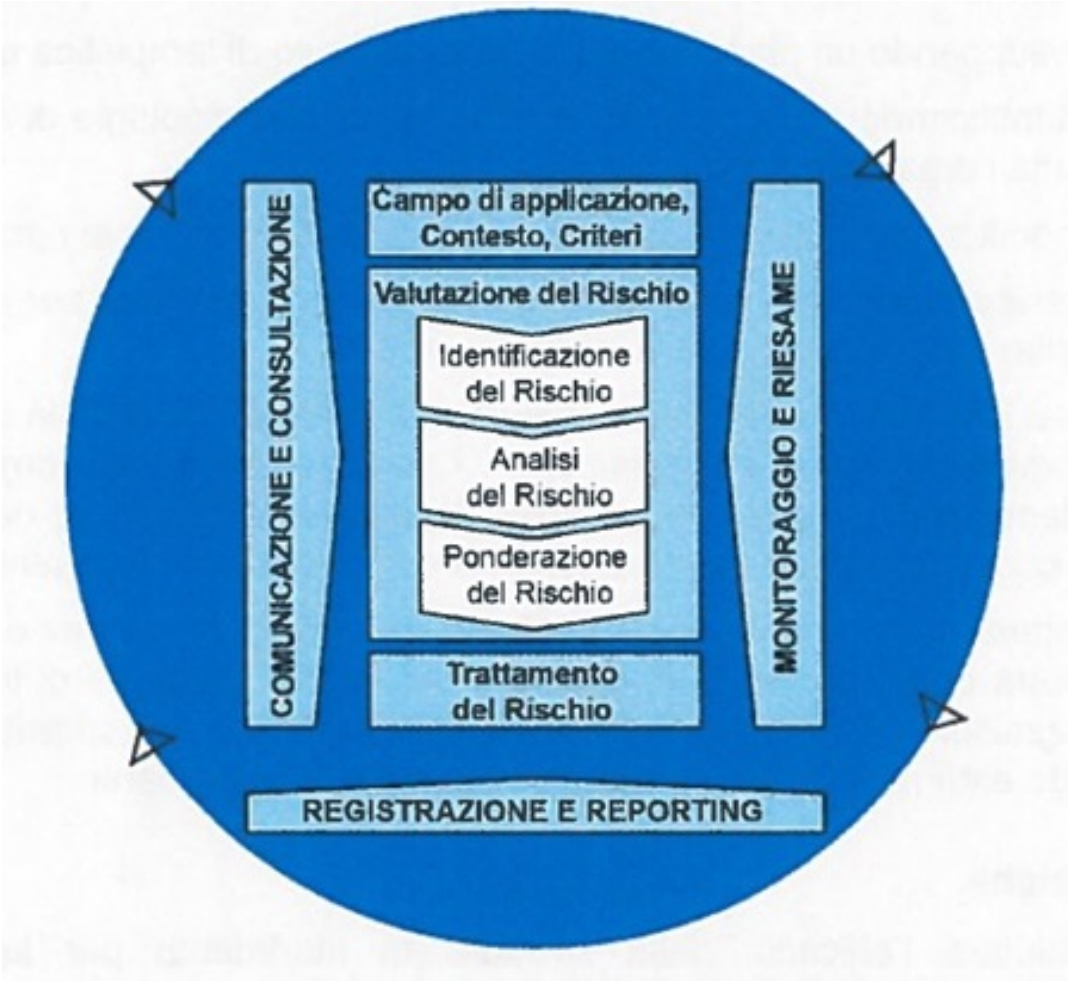
- Valutazione del rischio in poce parole:
  - Soppesa le tue capacità e le tue esigenze, usando
    - Assets principali
    - potenziali minacce
    - Controlli di sicurezza installati
  - Analizza lo stato attuale e i possibili miglioramenti
    - Sei contento dei rischi attuali?
    - Cosa puoi fare per migliorare il tuo livello di rischio
- Pros:
  - Risponde alle **tue** esigenze
  - Ottimizza le decisioni
  - Facile da capire e utilizzare dal gestore
  - Supporta la giustificazione delle decisioni prese
- Cons:
  - Richiede una buona conoscenza (e dati) sulla sicurezza cyber

8

VALUTAZIONE DEL RISCHIO E TERMINI RELATIVI

GESTIONE DEL RISCHIO

- **Gestione del rischio** – attività coordinata per dirigere e controllare un'organizzazione in relazione al rischio [ISO 31000]



PRINCIPI DI GESTIONE DEL RISCHIO

- Integrato
- Strutturato e completo
- Personalizzato
- Inclusivo
- Dinamico
- Le migliori informazioni disponibili
- Fattori umani e culturali
- Miglioramento continuo

VALUTAZIONE DEL RISCHIO

Valutazione del rischio – un sottoprocesso di gestione del rischio per l'identificazione, l'analisi e la ponderazione del rischio

TRATTAMENTO DEL RISCHIO

- La valutazione del rischio stima il livello attuale del rischio
  - Dove siamo?
- Il trattamento del rischio aiuta a pianificare i passaggi per affrontare i rischi eccessivi
  - Che cosa facciamo?
- L'implementazione di piu o migliori controlli è solo un modo (riduzione del rischio) per trattare i rischi!
  - Trattamento del rischio ≠ più controlli
  - Trattamento del rischio ⊃ più controlli
- I problemi individuati possono (e dovrebbero essere) risolti a livello di rischio, con altri strumenti (inclusi l'evitamento del rischio, il trasferimento del rischio e l'accettazione del rischio).

GESTIONE DELLA SICUREZZA

- In genere, la gestione della sicurezza è maggiormente focalizzata
  - sugli aspetti tecnici
  - sulla riduzione della probabilità del verificarsi di una minaccia
  - sull'aumento della forza della sicurezza.

- Non prende (esplicitamente) in considerazione il possibile impatto.
  - Gestione della sicurezza È governata dalle decisioni di gestione del rischio

- Ma la differenza con la gestione del rischio è sfumata e non è cruciale
  - Alcuni dicono addirittura che la gestione della sicurezza = gestione del rischio

STANDARD DI GESTIONE DEL

- Cyber Risk Management
  - ISO 31000 – Risk management – Guidelines
  - **ISO 27001 – Information security management systems — Requirements**
  - NIST 800-37 – Risk Management Framework for Information Systems and Organizations
- Cybersecurity framework
  - **NIST Cybersecurity Framework**
  - Framework Nazionale per la Cybersecurity e la Data Protection [Ita]
- Cyber Risk Assessment
  - ISO 27005 – Information security risk assessment
  - NIST 800-30 – Guide for Conducting Risk Assessments
  - Other risk management methodologies:
    - CIS RAM, OCTAVE, Magerit, Mehari, Microsoft, etc.
- Control lists:
  - ISO 27002 – Code of practice for information security controls
  - NIST 800-53 - Security and Privacy Controls
  - CIS Controls

15

VALUTAZIONE DEL RISCHIO CYBER

VALUTAZIONE DEL RISCHIO CYBER

- La valutazione del rischio è uno strumento **universale** per la gestione di qualsiasi tipo di rischio
- Allora, cos'è la valutazione del rischio **cyber**?
  - È l'applicazione del processo di valutazione del rischio universale al dominio cyber, tenendo conto delle peculiarità dell'ambiente cyber.
    - Come definire l'ambito del sistema di sicurezza cyber?
    - Quali sono le tipiche cyber assets?
    - Quali minacce sono tipiche dei rischi cyber?
    - Quali sono i controlli di sicurezza cyber?
    - Come stimare l'impatto?
    - Come stimare le probabilità e l'esposizione?

TIPICO PROCESSO DI VALUTAZIONE DEL RISCHIO

- Definizione del contesto
- Identificazione del rischio
  - Assets
  - Minacce
  - Controlli/vulnerabilita
- Stima/analisi del rischio
  - Impatto
  - Esposizione
  - Probabilità
  - Calcolo del rischio
- Ponderazione del rischio
  - Prioritizzazione del rischio
  - Ponderazione del rischio

DEFINIZIONE DEL CONTESTO. CONTESTO

- È necessario comprendere l'ambiente in cui opera il sistema IT e quanto influisce sulla valutazione del rischio

- In particolare, devono essere presi in considerazione i seguenti punti:
  - Obiettivi, strategie e politiche aziendali delle organizzazioni
  - Processo, funzione e struttura aziendale
  - Requisiti legali, normativi e contrattuali
  - L'approccio generale dell'organizzazione alla gestione del rischio
  - Posizione geografica
  - Aspettative degli stakeholder
  - Posizione e ambiente socio-culturale

DEFINIZIONE DEL CONTESTO. SCOPO E CONFINI

- Scopo
  - assicura che tutte le assets pertinenti siano prese in considerazione durante la valutazione del rischio.
- Confini
  - aiuta a concentrarsi sulle minacce che potrebbero penetrare attraverso i confini.
- Nel contesto cyber, è importante prestare particolare attenzione all'ambito e ai confini a causa della natura distribuita dei sistemi IT:
  - Il servizio cloud rientra nei tuoi confini o no?
  - Le assets sui dispositivi connessi dall'esterno della rete devono rientrare nell'ambito della valutazione?
  - Le assets sui dispositivi mobili connessi alla rete devono essere incluse nell'ambito?

DEFINIZIONE DEL CONTESTO. CRITERI

- Criteri di valutazione del rischio
  - Questi sono i criteri per valutare i rischi di sicurezza cyber, che includono:
    - Importanza strategica dei processi aziendali esistenti
    - Sensibilità degli asset cyber
    - Obblighi legali, regolamentari e contrattuali
    - In che modo la riservatezza, l'integrità e la disponibilità delle risorse cyber influiscono sui processi aziendali
    - Aspettativa degli stakeholder e valore della fiducia e della reputazione.
- Criteri di impatto
  - Questi i criteri per valutare l'eventuale perdita:
    - Violazioni (perdita di riservatezza, integrità, disponibilità)
    - Operazioni sospese
    - Scadenze mancate
    - Perdita finanziaria (compresa la perdita di opportunità commerciali)
    - Perdita di reputazione
    - Incapacità di adempiere ai requisiti legali, regolamentari e contrattuali

- Criteri di accettazione del rischio
  - Questi criteri definiscono quali livelli di rischio sono accettati
  - Potrebbe avere diversi livelli
  - Potrebbe essere diverso per diversi rischi
  - Potrebbe dipendere dal profitto atteso

IDENTIFICAZIONE DEL RISCHIO

IDENTIFICAZIONE DEL RISCHIO. CYBER ASSETS

- Peculiarità nell'identificazione degli asset cyber
  - Le cyber assets potrebbero essere difficili da assegnare a un oggetto fisico (ad esempio, i dati del cliente sono archiviati su un server), perché sono facili da copiare, modificare e scambiare (ad esempio, comunicati tramite Intranet/Internet, elaborati su un desktop; backup su un NAS o cloud, ecc.).
  - Le cyber assets sono difficili da monitorare. Potrebbero essere copiati su cyber risorses diverse. Potrebbero essere elaborati e trasformati in una risorsa diversa (ad es. analisi o registri).
  - Non è banale identificare ed elencare tutti le cyber assets. Spesso il valore delle cyber assets è troppo minato (ad esempio, informazioni di identificazione personale, come posizione o e-mail).
  - Alcuni cyber asset sono molto importanti, ma non provocano perdite immediate o definitive. Esempio: credenziali.
  - Esistono modi non standard (a volte innovativi) per gli aggressori di abusare delle vostre assets o usarle per attaccare gli altri. Ad esempio, cryptojacking, botnet o attacchi alla supply chain.
  - Le assets potrebbero dipendere l'una dall'altra (ad esempio, i dati sono necessari per eseguire un processo aziendale)

IDENTIFICAZIONE DEL RISCHIO. CYBER ASSETS

- Logico
  - Processi di business
  - Informazione
    - informazioni di identificazione personale,
    - informazioni sulla salute personale,
    - informazioni finanziarie
    - Competenza
    - Informazioni strategiche aziendali
    - Informazioni rilevanti per l'attività
  - Credenziali
  - Codice sorgente
- Contenitrici
  - Banche dati
  - File
  - Applicazioni
  - Comunicazione
  - E-mail
  - L'ambiente del sviluppo
  - Servizio web/sito web
- Fisico
  - server
  - Rete
  - Personale
  - IoT, dispositivo mobile
  - Desktop
  - Supporti (CD, NAS, ecc.)
  - Cloud
  - Carta

IDENTIFICAZIONE DEL RISCHIO. MINACCE

- Le minacce cyber sono, in gran parte, intenzionali. Il che significa che combattiamo contro altri umani:
  - Adattabile
  - Inventivo
  - Collaborativo
  - Pianificante
  - Paziente
  - Potrebbe essere persistente
- Le minacce cyber sono eterogenee e dinamiche
  - Compaiono nuove minacce
  - Le minacce esistenti si evolvono
  - Riappaiono vecchie minacce.

IDENTIFICAZIONE DEL RISCHIO. MINACCE

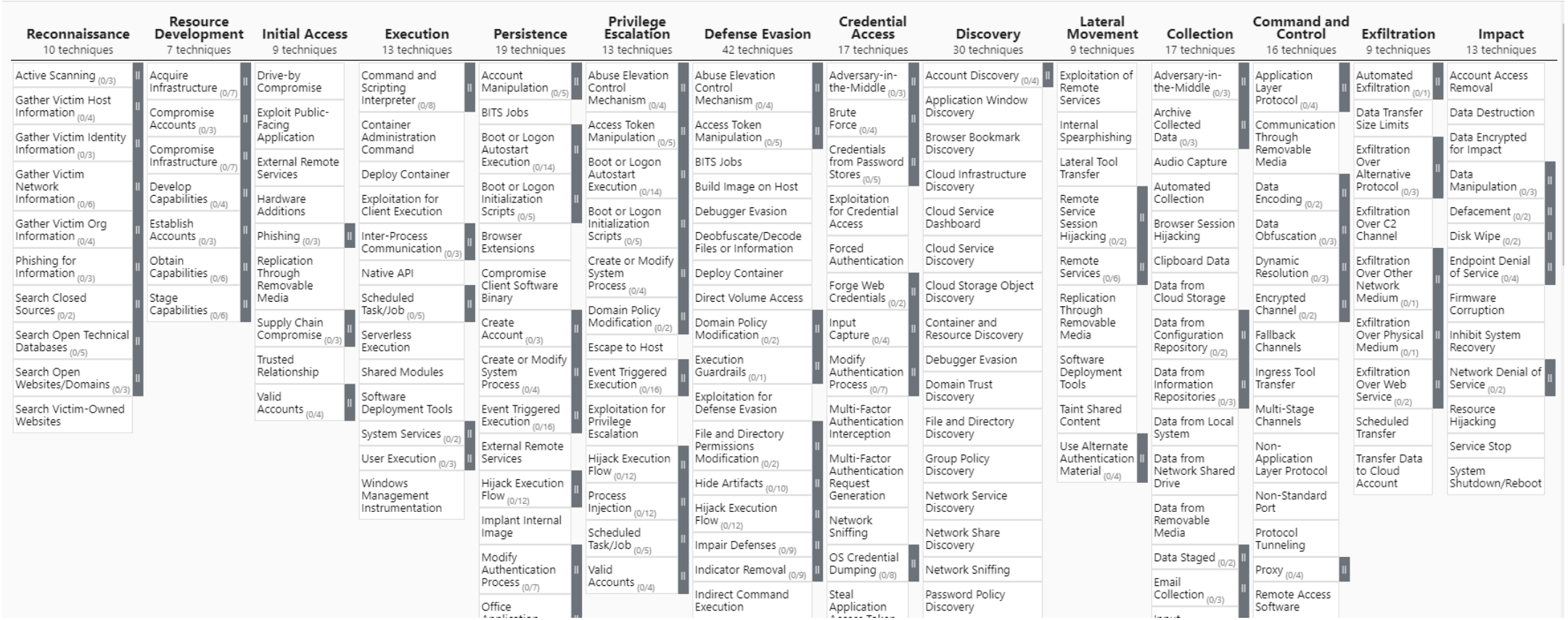
- Gli attacchi cyber spesso richiedono diversi passaggi per ottenere il risultato.
  - Un utente apre un'e-mail fraudolenta con un virus allegato.
  - Un virus viene eseguito sul dispositivo di una vittima. È installata una backdoor
  - Un attaccante ottiene l'accesso al sistema ed esegue un exploit per ottenere un accesso di livello superiore
  - E…
    - Rubare dati?
    - Implementare un bot? criptojacker?
    - Ottenere l'accesso a un server?
    - Piantare un ransomware?

- Vengono utilizzate diverse vulnerabilità
- Si verificano diverse minacce
- L'esito finale (impatto) è incerto.

IDENTIFICAZIONE DEL RISCHIO. SCENARI

- Una possibile soluzione: definire gli scenari.
- Uno scenario è un modo specifico per attaccare un sistema e ottenere determinati risultati. Aiuta a chiarire:
  - Chi è l'aggressore
  - Quali vulnerabilità vengono sfruttate
  - Qual è l'impatto previsto.
- In questo caso è possibile capire
  - Quali controlli possono impedirlo
  - Quale assets sono interessati e in che modo l`attackante gli puo compromettere.
- Ma
  - C'è (quasi) una quantità infinita di scenari
  - Non ci sono (quasi) statistiche disponibili per gli scenari
  - La maggior parte dei dati statistici disponibili si concentrano sulle minacce.

MITTRE ATT&CK MATRIX



Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 13 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/3)	Acquire Infrastructure (0/7)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Adversary-in-the-Middle (0/3)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Compromise Accounts (0/3)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/7)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	BITS Jobs	Credentials from Password Stores (0/5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (0/3)	Phishing (0/3)	Inter-Process Communication (0/3)	Browser Extensions	Create or Modify System Process (0/4)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (0/6)	Browser Session Hijacking	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (0/2)	Deobfuscate/Decode Files or Information	Forge Web Credentials (0/2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)	Stage Capabilities (0/6)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/5)	Create Account (0/3)	Escape to Host	Deploy Container	Input Capture (0/4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Fallback Channels	Exfiltration Over Web Service (0/2)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)		Trusted Relationship	Serverless Execution	Create or Modify System Process (0/4)	Event Triggered Execution (0/16)	Direct Volume Access	Modify Authentication Process (0/7)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (0/2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (0/3)		Valid Accounts (0/4)	Shared Modules	Event Triggered Execution (0/16)	Exploitation for Privilege Escalation	Domain Policy Modification (0/2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Software Deployment Tools	External Remote Services	Hijack Execution Flow (0/12)	Execution Guardrails (0/1)	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service (0/2)
			System Services (0/2)	Hijack Execution Flow (0/12)	Process Injection (0/12)	Exploitation for Defense Evasion	Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
			User Execution (0/3)	Implant Internal Image	Scheduled Task/Job (0/5)	File and Directory Permissions Modification (0/2)	OS Credential Dumping (0/8)	Group Policy Discovery		Data from Removable Media	Protocol Tunneling		Service Stop
			Windows Management Instrumentation	Modify Authentication Process (0/7)	Valid Accounts (0/4)	Hide Artifacts (0/10)	Steal Application	Network Service Discovery		Data Staged (0/2)	Proxy (0/4)		System Shutdown/Reboot
				Office		Hijack Execution Flow (0/12)		Network Share Discovery		Email Collection (0/3)	Remote Access Software		
						Impair Defenses (0/9)		Network Sniffing					
						Indicator Removal (0/9)		Password Policy Discovery					
						Indirect Command Execution							

IDENTIFICAZIONE DEL RISCHIO. ATTACCANTI

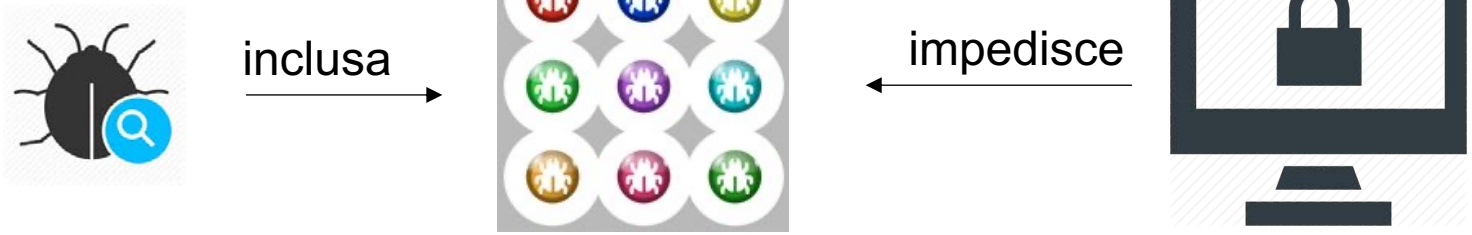
- Attaccante esterno
  - Criminale cyber
  - Cyber terrorista / nazione sponsorizzata
  - Virus/worm
  - Hacktivista
  - Spia industriale
- Attaccante interno
  - Abusatore
  - Hacker
- Cliente malizioso
- Attaccante fisico
- Fornitore
- Utente negligente
- Fallimenti
- Ambiente
  - Locali (inquinamento, riscaldamento, ecc.)
  - Globali (terremoto, alluvione, ecc.)

IDENTIFICAZIONE DEL RISCHIO. MINACCE

- Gli attaccanti possono essere caratterizzati da
  - Obiettivi
  - Capacità
  - Bersaglio
- Gli attaccanti eseguono le loro attività attraverso minacce o scenari
- Per riassumere: un attaccante esegue una minaccia/scenario specifico per sfruttare le vulnerabilità del sistema per realizzare il suo obiettivo compromettendo asset specifici (bersaglio)
  - Una **minaccia/scenario** definisce/lega le **vulnerabilità** da sfuttare e le **assets** da compromettere

VULNERABILITÀ VS CONTROLLI DI SICUREZZA

- Semplificazione dell'identificazione delle vulnerabilità:
  - Mancanza di controlli di sicurezza = una vulnerabilità



Bug specifico	Tipo di bug	Controllo di sicurezza
Basso livello Tecnico Difficile ragionare	Alto livello Generico Ragionamento più semplice	“Facile” da identificare Generico Elencato negli standard (ISO 27002, CSF, CIS)

TIPICHE MINACCE CYBER

VIRUS, WORM AND RANSOMWARE

- **Virus** e **worm** sono programmi dannosi che possono modificare il funzionamento e il comportamento del computer. Virus e worm hanno meccanismi di propagazione diversi.
  - Virus. Un utente dovrebbe consentire l'esecuzione di un virus. Per esempio,
    - Aprire un allegato di posta dannoso
    - Consentire l'installazione di un programma infetto
    - Scaricare ed esegui un file infetto
  - Il worm si propaga autonomamente sfruttando le vulnerabilità nei servizi di rete.
- Il **ransomware** è un malware che crittografa i dati del computer compromesso, rendendo inutilizzabili i file e il sistema. Di solito, dopo viene richiesto un riscatto all'utente.
  - Distribuito in modi diversi, inclusi virus e worm, ma può anche essere installato da un utente malintenzionato che dispone di diritti di accesso sufficienti sul computer.

ATTACCHI BASATI SUL WEB ATTACCHI ALLE APPLICAZIONI WEB

- **Attacchi alle applicazioni Web**: un'ampia gamma di attacchi volti a sfruttare le vulnerabilità nella GUI e nelle API del servizio (ad esempio, attacchi SQL injection, Cross-Site scripting XSS). Mira a compromettere le applicazioni web.

- **Attacco basato sul Web**: un'ampia serie di attacchi durante i quali gli aggressori sfruttano le vulnerabilità nella codifica per ottenere l'accesso a un server o un computer. Mira a compromettere un sistema connesso a Internet.

ATTACCHI ALLA COMUNICAZIONE D(DOS)

- **Attacco alla comunicazione**: questa minaccia mira a intercettare o manomettere la comunicazione tra una vittima. L'attaccante può trovare un modo per decifrare la comunicazione (con crittografia assente o debole) o sfruttare le vulnerabilità dei protocolli non sicuri
  - Man in the middle attacca: un utente malintenzionato interrompe la comunicazione tra due vittime e costringe il traffico a fluire attraverso di lui, con la possibilità di leggere o modificare la comunicazione.

- **(D)DoS**: la minaccia Denial of Service mira a bombardare il servizio selezionato con un'enorme quantità di richieste che rendono il servizio non disponibile per gli utenti legittimi
  - (Distribuito) Denial of Service utilizza una moltitudine di fonti (bot) che inviano richieste al servizio.

ATTACCHI DI INGEGNERIA SOCIALE. ATTACCHI FISICI

- **Ingegneria sociale**: è una serie di minacce che mirano a manipolare, influenzare e ingannare una vittima al fine di indurla ad agire in un certo modo (ad esempio, concedere l'accesso a un sistema cyber, condividere informazioni segrete o credenziali).
  - *Phishing*: una tipica minaccia di ingegneria sociale che comunica con un utente tramite e-mail, messenger o altri mezzi di comunicazione.
  - Gli attacchi di ingegneria sociale richiedevano la presenza fisica
    - *Shoulder surfing*: sbirciare la digitazione della password
    - *Dumpster diving*: cercare le password nella lettiera
    - *USB drop*: lasciare che una chiavetta USB infetta venga prelevata e utilizzata da un dipendente
- **Attacchi fisici**: danni intenzionali all'hardware causati da aggressori (interni o esterni)
- **Manomissione**: modifica fisica di un hardware per alterarne la funzionalità o ottenere l'accesso alla rete.

INSIDER
PARTNER/FORNITORE

- **Abuser**: un dipendente utilizza i propri diritti di accesso per compromettere il sistema. Per esempio, copiare i dati all'esterno della sede dell'azienda.

- **Insider hacker**: un utente malintenzionato che beneficia dell'accesso iniziale al sistema ma mira ad aumentare i propri privilegi compromettendo il sistema.

- **Ex dipendente** – un ex dipendente, che utilizza la propria conoscenza del sistema, credenziali ancora valide e/o backdoor precedentemente installate per comprometterlo.

- **Partner** – un partner che attacca il sistema, usando i suoi privilegi nel tuo sistema
  - Un partner potrebbe essere compromesso. L'hacker può mirare ad attaccare il tuo partner per usarlo come punto d'appoggio per attaccarti: attacco alla catena di approvvigionamento.

CLIENTE DANNOSO

- **Cliente dannoso**: un client che utilizza i servizi acquistati per lanciare un attacco a te o ai tuoi clienti

- **Cliente illegale**: un cliente che utilizza il tuo servizio per scopi illegali (ad esempio, inviare spam, ospitare contenuti illegali, fornire servizi dannosi, ecc.).

NEGLIGENZA DEL DIPENDENTE

- **Perdita o furto dell'hardware**: una minaccia correlata alla perdita fisica di un hardware. Questa minaccia in genere si traduce in una potenziale perdita di informazioni sensibili contenute su un dispositivo mobile (ad esempio, laptop o cellulare).
- **Danni fisici accidentali**: un'azione accidentale di un dipendente che causa danni fisici all'hardware. Ad esempio, caffè versato su un laptop.
- **Errore logico accidentale**: un errore accidentale o un'azione benigna che porta a compromettere il sistema. Un errore tipico è la condivisione di dati sensibili (ad esempio, concedendo l'accesso a dati sensibili al pubblico o condividendo informazioni senza sapere che sono private).

MINACCE AMBIENTALI GUASTI

- **Locale** – minacce ambientali che colpiscono solo la rete dell'impresa (inquinamento, riscaldamento, acqua, fuoco, polvere, impulsi elettromagnetici, ecc.)
- **Globale** – eventi naturali che danneggiano una vasta area (terremoto, alluvione, attività vulcanica, ecc.)
- **Glitch del sistema**: un errore accidentale nel funzionamento del sistema IT, che causa danni.
- **Guasto meccanico** - guasto meccanico che causa danni.

CONTROLLI DI SICUREZZA

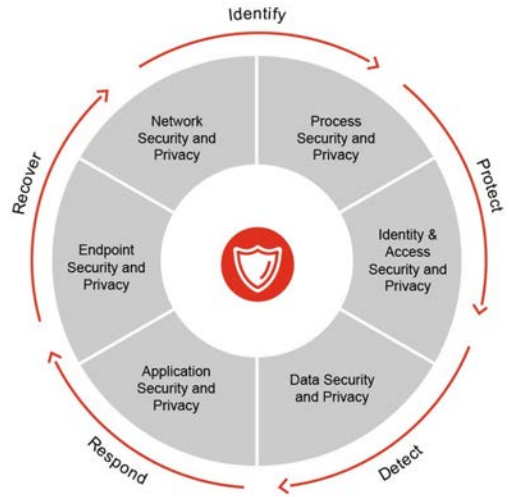
CONTROLLI DI SICUREZZA. ISO 27002 VS CSF

ISO

- Organizzazione
- Politiche
- Gestione delle assets
- Conformità
- Rapporti con i fornitori
- Protezione fisica e ambientale
- Risorse umane
- Controllo di accesso
- Crittografia
- Sicurezza della comunicazione
- Sicurezza operativa,
- Acquisizione, sviluppo e manutenzione del sistema
- Gestione degli incidenti
- Business continuity

NIST CSF

- Identificare
  - Gestione delle Asset, Organizzazione, Policy, Rapporti con i fornitori, Compliance
- Proteggere
  - Protezione fisica e ambientale, Risorse umane, Controllo degli accessi, Sicurezza delle operazioni, Crittografia, Sicurezza delle comunicazioni, Acquisizione, sviluppo e manutenzione del sistema
- Rilevare
  - Protezione del sistema
- Rispondere
  - Gestione degli incidenti
  - Business continuity
- Recuperare
  - Gestione degli incidenti



POLITICHE

- Un insieme di politiche per la sicurezza cyber dovrebbe essere:
  - Definito
  - Approvato (dalla direzione)
  - Pubblicato
  - Comunicato ai dipendenti e ai soggetti esterni
  - Revisionato regolarmente

ORGANIZZAZIONE

- Definire ruoli e responsabilità
- Stabilire contatti con le autorità
- Definire le politiche per l'uso dei dispositivi mobili e il telelavoro

RISORSE UMANE

- Eseguire lo screening dei candidati
- Definire contrattualmente termini e condizioni in materia di sicurezza cyber
- Rendere la gestione per garantire che le politiche di sicurezza siano seguite
- Formare e formare i dipendenti
- Istituire un processo disciplinare
- Assicurarsi che la procedura di risoluzione del contratto includa le azioni di sicurezza richieste

GESTIONE DELLE ASSETS

- Creare, mantenere e aggiornare l'inventario delle risorse
- Definire il proprietario delle risorse
- Classificare le risorse
- Gestire supporti rimovibili
- Smaltimento sicuro dei supporti
- Transizione sicura dei supporti fisici

CONTROLLO DI ACCESSO

- Definisci criteri per il controllo degli accessi (in particolare, l'accesso alla tua rete IT)
- Definire come registrare e annullare un utente
- Definire formalmente in che modo viene concesso o revocato l'accesso
- Gestione speciale dei diritti di accesso privilegiato
- Specificare un processo di gestione formale per la gestione delle informazioni di autenticazione segrete e assicurarsi che gli utenti lo seguano.
- Definire le regole formali per la rimozione o la modifica dei diritti di accesso
- Assicurarsi che l'accesso sia concesso in base alle politiche di controllo degli accessi
- Stabilire procedure di accesso sicure e sistemi di gestione delle password
- Limitare l'accesso al codice sorgente.

CRITTOGRAFIA

- Definire i criteri per l'utilizzo dei controlli crittografici

- Definire le politiche per la gestione delle chiavi
  - Come usare
  - Come proteggere
  - Durata delle chiavi crittografiche

PROTEZIONE FISICA E AMBIENTALE

- Stabilire e proteggere il perimetro fisico
- Stabilire controlli fisici
  - Uffici sicuri e altre strutture
- Stabilire procedure per lavorare in aree sicure
- Definire e implementare le procedure per la consegna e il carico
- Implementare protezioni contro disastri naturali, attacchi e incidenti dannosi.
- Proteggere e mantenere apparecchiature, utenze, cavi, ecc.
- Definire e seguire le procedure per lo smaltimento e la rimozione delle apparecchiature.
- Definire politice clear desk e clear screen.

SICUREZZA DELLE OPERAZIONI

- Definire le procedure operative e le responsabilità
- Implementa la protezione da malware
- Implementare procedure di backup
- Implementare procedure di registrazione e monitoraggio
- Procedure definite per l'installazione di un software
- Implementare le procedure di gestione delle vulnerabilità
- Pianificare le attività di audit

SICUREZZA DELLA COMUNICAZIONE

- Definire le procedure di gestione per il controllo della rete
- Implementare e mantenere i meccanismi di sicurezza della rete (ad es. firewall, IDS/IPS, ecc.)
- Segregare le reti (se necessario).
- Definire come e quali informazioni possono essere trasferite
- Definire le regole per la messaggistica elettronica
- Definire i requisiti per gli accordi di riservatezza e non divulgazione per lo scambio di informazioni.

ACQUISIZIONE, SVILUPPO E MANUTENZIONE DEL SISTEMA

- Definire e implementare i requisiti di sicurezza per i nuovi sistemi informativi (in particolare, come le applicazioni scambiano informazioni nelle reti pubbliche)
- Definire regole per uno sviluppo sicuro
- Definire e implementare il controllo sulle modifiche ai sistemi
- Utilizzare i principi di ingegneria del sistema sicuro
- Ambiente di sviluppo sicuro
- Definire le regole per lo sviluppo in outsourcing
- Utilizzare i test di sicurezza e di accettazione del sistema

RAPPORTI CON I FORNITORI

- Definire le politiche di sicurezza per i fornitori
- Garantire che i requisiti di sicurezza siano negoziati, concordati e rispettati dal fornitore
- Rivedere e monitorare l'adempimento dei requisiti di sicurezza da parte del fornitore.

GESTIONE DEGLI INCIDENTI DI SICUREZZA DELLE INFORMAZIONI

- Definire le responsabilità e le procedure per la risposta all'incidenza e garantire la loro esecuzione
- Stabilire procedure di segnalazione per eventi e debolezze
- Garantire che gli eventi di sicurezza vengano analizzati e valutati.
- Garantire l'esecuzione delle procedure per la risposta agli incidenti
- Analizzare gli eventi accaduti e applicare azioni per riduzione dei rischi simili in futuro
- Memorizza le informazioni sugli eventi verificatisi.

BUSINESS CONTINUITY

- Definire i requisiti per, pianificare, implementare, rivedere le procedure di continuità operativa.

CONFORMITÀ

- Identificare le legislazioni e gli accordi contrattuali necessari per conformarsi
- Identificare i diritti di proprietà intellettuale e proteggerli
- Proteggi i dati di terze parti in conformità con la legge (ad es. GDPR)
- Seguire le normative sui controlli crittografici

AUDIT

- Organizza una revisione indipendente del tuo sistema di sicurezza cyber
- Garantire la conformità con le politiche o gli standard di sicurezza

STRUMENTI E METODI

RICERCA DESKTOP

- Analisi dei documenti aziendali
  - Strategia aziendale, Strategia aziendale, Diagrammi di flusso, Assegnazione ruoli,…
  - Raporti di valutazione del rischi precedenti
  - Inventario delle risorse
  - Analisi dei log, analisi degli eventi passati, report (compresi i report di audit)…
  - Rapporti sulla scansione delle vulnerabilità (Nessus, OpenVas)
- Fonti esterne
  - Analisi statistiche (ENISA, IBM/Ponemon, Verizon, Accenture, NetDilligence, McAffee, Semantec, Deloitte, PwC, ecc…)
  - Rapporti, bollettini dei centri di condivisione delle informazioni (ad es. CERT, ISACs).
- Aggregazione di fonti diversi:
  - Valore medio
  - Weighted function:
    - $X = \sum_{\forall i} w_i \times x_i$

PARLARE CON LA GENTE

- **Interviste**: discussioni individuali con le principali parti interessate sullo stato attuale della pratica (responsabili della sicurezza, risorse umane, proprietari delle risorse, ecc.)
- **Workshop**: discussioni di gruppo con le persone coinvolte nella valutazione del rischio
- **Metodo Delphi** : un metodo di previsione sistematico e interattivo che si basa sull'opinione presa in considerazione di diversi esperti
  - Gli esperti rispondono a un questionario (fornendo spiegazioni)
  - Le risposte sono segnalate in forma anonima ad altri (con spiegazioni)
  - Gli esperti rispondono nuovamente al questionario (correggendo le risposte)
  - Fermati a un criterio predefinito (ad esempio, numero fisso di giri) e viene utilizzato il punteggio medio o medina.

AGGREGAZIONE DI DATI DAI FONTI DIVERSI:

- Mediana

  {2,4,**5**,8,8}

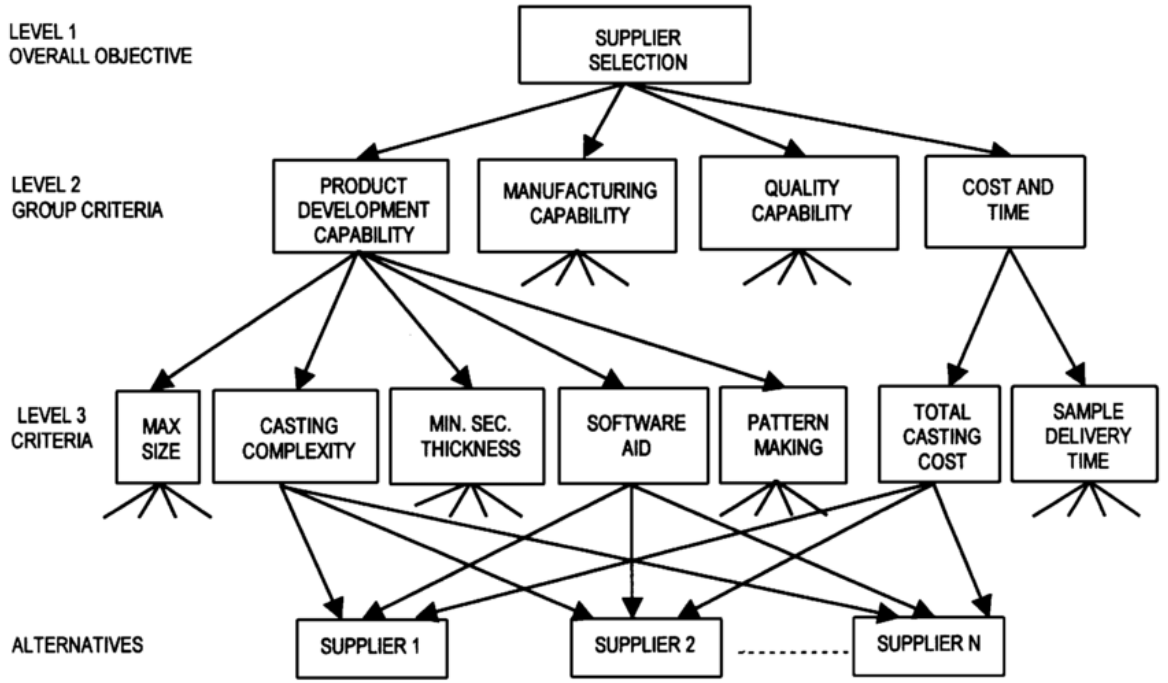
- Valore medio

$$X = \frac{1}{n}\sum_{i=1}^{n} x_i$$

- Weighted function:

$$X = \sum_{\forall i} w_i \times x_i$$

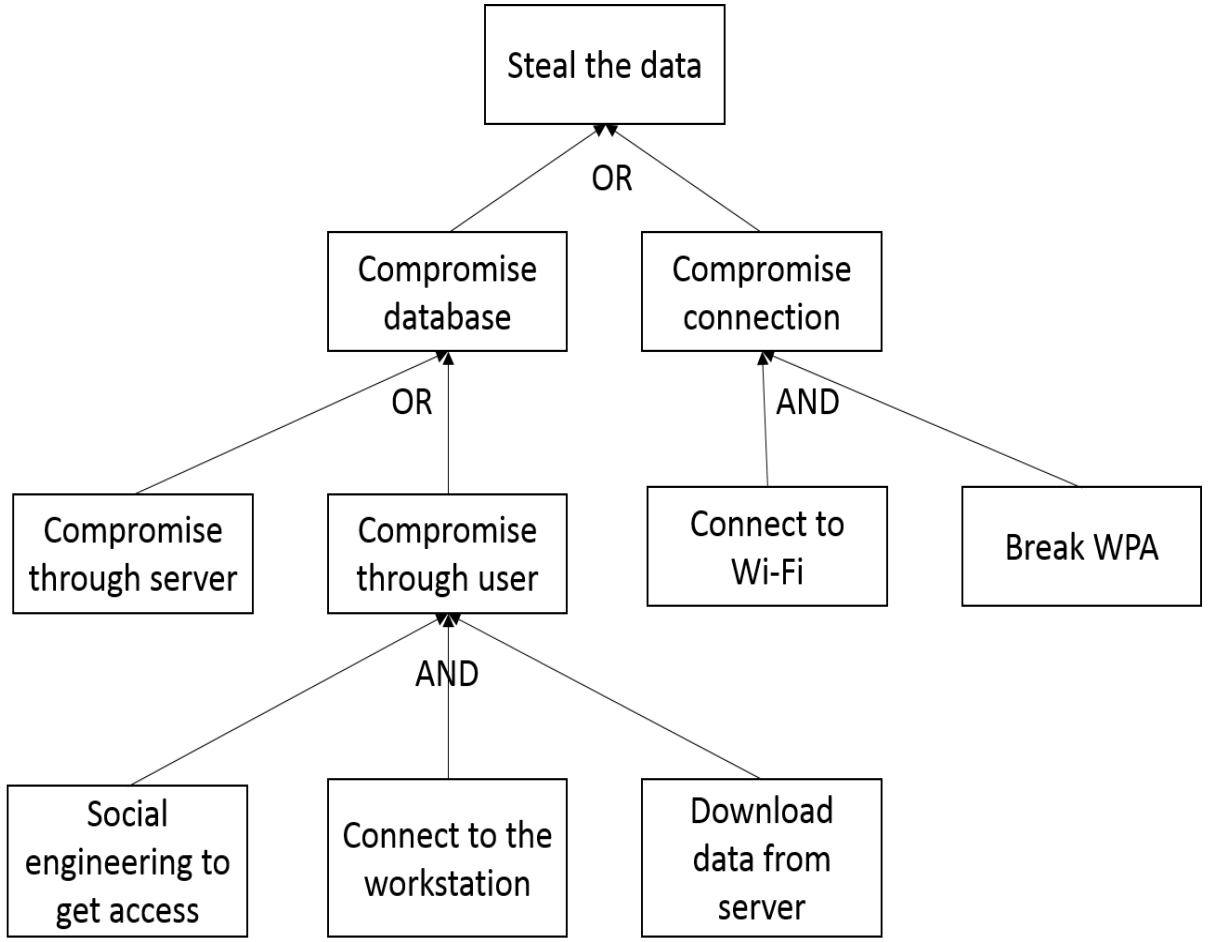
- Analytic Hierarchy Process (AHP)



ATTACK TREE

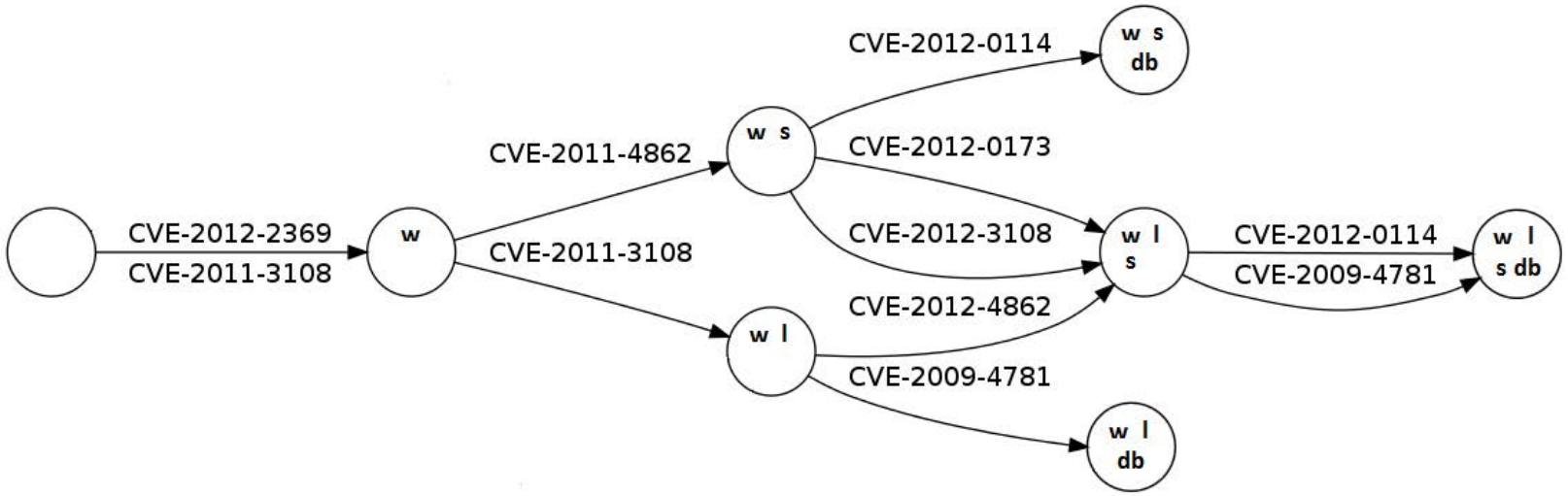
- Attach tree è una tecnica utile per un modo strutturato per analizzare e dettagliare le minacce

- Inizia con una possibile conseguenza indesiderata (nodo superiore)
- Suddividilo usando gli operatori AND e OR in passaggi più dettagliati
- Ripetere fino a raggiungere il livello di dettaglio richiesto.



ATTACK GRAPH

- Attack graph è una tecnica che mira a rappresentare tutti i percorsi (una sequenza di vulnerabilità esistenti da sfruttare) attraverso un sistema che un utente malintenzionato può seguire per raggiungere il suo obiettivo finale.
- Dopo la scansione delle vulnerabilità, lo strumento di creazione del attack graph li collega in un grafico basato sulle condizioni pre e post per ogni vulnerabilità rilevat



ANALISI E PONDERAZIONEDEL RISCHIO

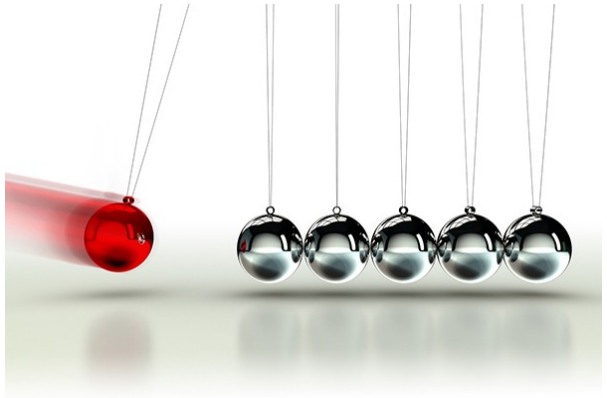
ANALISI DEL RISCHIO QUANTITATIVA O QUALITATIVA

- Quantitativo
  - Funziona con valori reali!
  - Le operazioni sui valori sono definite.
  - Fornire risultati monetari (adatti per ulteriori analisi e riutilizzo)
  - Difficile da usare
- Perdita – misurata in euro [dollari, tugrik, ecc.]
- Likelihood: valore reale positivo

- Qualitativo
  - Facile da applicare
  - Ampiamente usato
  - Ha bisogno della definizione di valore
  - Necessita della definizione delle operazioni
- Perdita – {very low, low, medium, high, very high}
- Likelihood – {very low, low, medium, high, very high}

ANALISI DEL RISCHIO. IMPATTO

- Una risorsa compromessa provoca la perdita.
  - L'impatto è stimato come una perdita attesa da un singolo evento di minaccia
- Tenere in considerazione:
  - Interruzione delle attività business
  - Perdita diretta
  - Violazione di una normativa
  - Violazione di un contratto
  - Perdita di reputazione
  - Perdita del cliente
  - Costo della notifica
  - Impatto sul personale/utente
  - Indagine/recupero perdita
  - Perdita di vantaggio competitivo
- Non dimenticare la dipendenza dalle risorse!



ANALISI DEL RISCHIO. IMPATTO

- Dal punto di vista della sicurezza è importante valutare le perdite dovute all'impatto su uno specifico aspetto della sicurezza:
  - Confidenzialità
  - Integrità
  - Disponibilità
- Potrebbe anche essere aggiunto
  - Responsabilità (non ripudio)

ANALISI DEL RISCHIO. LIKELIHOOD

- Likelihood = Esposizione × Probabilità[Successo]
  - Fonti di minaccia e contesto organizzativo
  - Controlli e vulnerabilità
  - Esperienza e statistiche

- L'esposizione è prevalentemente esterna
  - Interessato dalle tendenze globali e dal tipo di organizzazione
- La probabilità è per lo più interna
  - Colpito dalla tua protezione

STIMA DEL RISCHIO. CALCOLARE

- Formula generale:
  - Rischio = Likelihood × Perdita

- Minacce multiple (t) e assets (a):
  - Per asset: $Rischio_{CIA}^{a} = \sum_{\forall\, t} Likelihood^{t} \times Impact_{CIA}^{a}$
  - Per minaccia: $Rischio_{CIA}^{t} = \sum_{\forall\, a} Likelihood^{t} \times Impact_{CIA}^{a}$

RISK ESTIMATION. COMPUTE RISK. QUALITATIVE

	Likelihood	**Very low**	**low**	**medium**	**high**	**Very high**
Perdita	**Very low**	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very high	4	5	6	7	8

PRIORITIZZARE I RISCHI

Assegnare priorità ai rischi in base a criteri di valutazione.

Minacce	Perdita	Likelihood	Rischio	Rank
Minaccia A	Very low	Very low	0	5
Minaccia B	Very high	Medium	6	1
Minaccia C	Low	Low	2	4
Minaccia D	Very low	High	4	2
Minaccia E	Medium	Low	3	3
Minaccia F	High	Low	4	2

VALUTAZIONE DEL RISCHIO. ESEMPIO 1

Risk Analysis	Value
Information Asset	Diary device controllers
CIS Control	15.9
Description	Disable wireless peripheral access of devices (such as Bluetooth and NFC), unless such access is required for a business purpose.
Control	Each diary device is joined to the diary device controller using a one-time, six-digit code that is displayed on the controller and entered at the device. At this point, all file transfers and firmware updates between devices are enabled.
Vulnerability	Diary device controllers are using a deprecated version of Bluetooth to support older diary devices. Bluetooth devices can manipulate Bluetooth services on the diary device controllers to gain access to files and commands on the controllers.
Threat	Hackers may walk through clinics with Bluetooth devices that are prepared to hack diary device controllers using attacks such as Blueborne, and may access hundreds of patient data files, as well as firmware.
Threat Likelihood	3
Mission Impact	3
Objectives Impact	4
Obligations Impact	2
Risk Score	**12**
Risk Acceptability	**Not Acceptable**

[CIS Risk Assessment Method]

VALUTAZIONE DEL RISCHIO. ESEMPIO 2

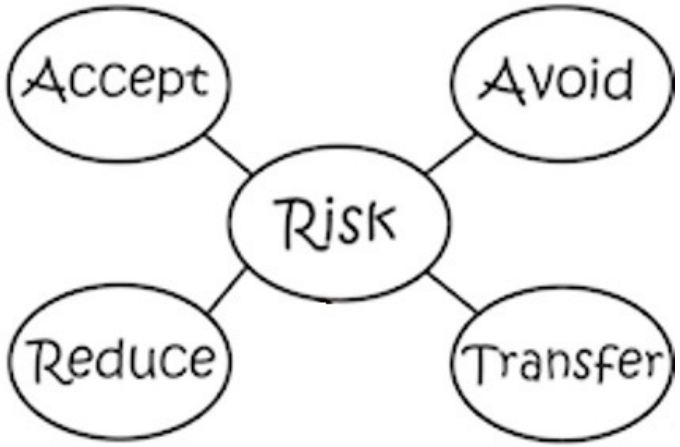
1	2	3	4	5	6	7	8	9	10	11	12	13
Threat Event	Threat Sources	Threat Source Characteristics			Relevance	Likelihood of Attack Initiation	Vulnerabilities and Predisposing Conditions	Severity and Pervasiveness	Likelihood Initiated Attack Succeeds	Overall Likelihood	Level of Impact	Risk
		Capability	Intent	Targeting								

[NIST 800-30 rev 1. Guide for Conducting Risk Assessments]

TREATMENTO DEL RISCHIO

TRATTAMENTO DEL RISCHIO

- Evitamento del rischio
  - non svolgere attività rischiose
- Mitigazione del rischio (riduzione)
  - Prevenire/ridurre il likelihood o la perdita di minac
- Trasferimento del rischio
  - Assicurazione e outsourcing
- Accettazione del rischio (ritenzione/tolleranza)
  - Allora… ok.



TRATTAMENTO DEL RISCHIO. RIDUZIONE

- Il rischio può essere ridotto in 3 modi:

- Ridurre l'esposizione alle minacce
  - Molto difficile!
  - Non irritare le gente.

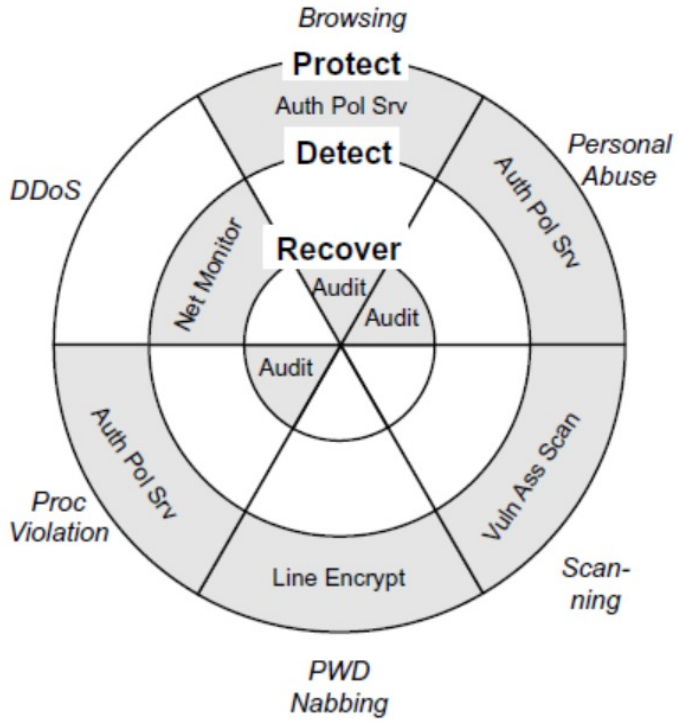
- Ridurre la probabilità di minaccia
  - Protezione da malware, protezione della rete, crittografia, gestione degli incidenti

- Ridurre l'impatto delle minacce
  - Piano di continuità operativa, Back-up, Gestione degli incidenti

TRATTAMENTO DEL RISCHIO. RIDUZIONE

- Difesa in ampiezza contro difesa in profondità
  - Livello di rete
    - Perimetro, reti, nodi finali

- Livello di sicurezza:
  - Prevenire, rilevare, monitorare, recuperare



- S. Butler "Security attribute evaluation method: a cost-benefit approach". International Conference on Software Engineering, 2002

TRATTAMENTO DEL RISCHIO. COST-BENEFIT ANALYSIS

- Cost benefit analysis
  - $Benefit = Risk_{before} - Risk_{after} - Cost$
- Return on (security) investment
  - $RO(S)I = \frac{Risk_{before} - Risk_{after}}{Cost}$
  - Greedy approach

- Scelte multiple? Possibile soluzione: soluzione a un problema simile a knapsack problem:
  - Selezionare una serie di possibili controlli per
    1. Riduci al minimo il rischio
    2. Mantieni i costi entro il budget

RISK TREATMENT. TRADE-OFF ANALYSIS. SEMI-QUANTITATIVE

		Tradeoff Attributes				
		Ease of Maintenance	Purchase Cost	Vulnerability	Productivity Impact	Tradeoff Ranking
Security Technology	Rank	w = .10	w = .25	w = .35	w = .30	$\Sigma w_i v_i(x_i)$
	Vulnerability Assessment Scanner	25	25	40	0	.20
	Secure Email	40	35	20	0	.24
	Smart Card	25	15	30	60	.34
	E-Signature	10	25	10	40	.22

- S. Butler "Security attribute evaluation method: a cost-benefit approach". International Conference on Software Engineering, 2002

TRATTAMENTO DEL RISCHIO. TRASFERIMENTO DEL RISCHIO

- Spostare l'attività a un'altra entità (responsabile della gestione del rischio)
  - Sicurezza gestita
  - Cloud
  - Sviluppo in outsourcing
- Ma è difficile trasferire la responsabilità

- Assicurazione
  - Acquista un'assicurazione per coprire quei rischi che non puoi accettare

PERCHÉ L'ASSICURAZIONE CYBER?

- L'assicurazione cyber è apparsa perché:
  - La vulnerabilità è aumentata a causa dell'espansione della tecnologia dell'informazione
  - Le minacce cyber causano grandi rischi aziendali
  - La mitigazione del rischio non elimina completamente il rischio
  - Gli approcci dei gestori del rischio devono essere integrati
- Benefici previsti:
  - Livellamento delle perdite
  - Servire come indicatore della qualità della protezione
  - Incentivo a investire in sicurezza
  - Aumento del benessere sociale
  - Provocare la comparsa di standard di sicurezza avanzati

TRATTAMENTO DEL RISCHIO. EVITAMENTO DEL RISCHIO

1. Cerca di ridurre il rischio
2. Prova a trasferirlo
3. Se il rischio è ancora troppo alto per accettarlo...
4. Chiudere l'attività soggetta a questo rischio.

- Per esempio,
  - non utilizzare un sistema cloud (ad esempio, se non hai le competenze per configurarlo correttamente) o
  - non esternalizzare la codifica a sviluppatori sconosciuti

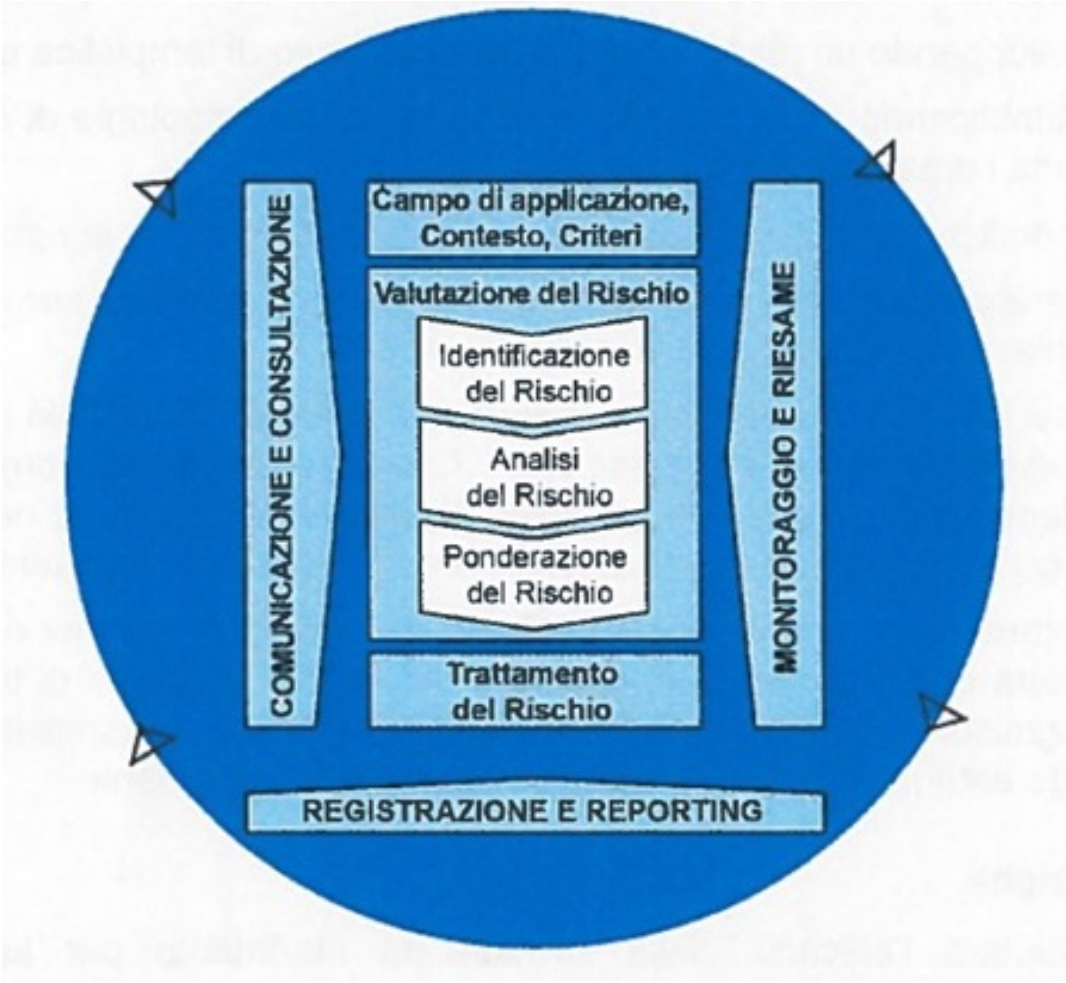
TRATTAMENTO DEL RISCHIO. ACCETTAZIONE DEL RISCHIO

- Opzione predefinita, ma devi essere consapevole di questa decisione
- Guidato da criteri di accettazione
- Possiamo essere coperti dall'autoassicurazione

- Se non puoi accettare il rischio, ripianifica il piano di trattamento del rischio

GESTIONE DEL RISCHIO. ALTRE ATTIVITÀ

- Comunicazione e Consultazione
  - Comunicare con le parti interessate
  - Consultare esperti esterni
- Monitoraggio e riesame
  - Monitorare i valori definiti
  - Esaminare regolarmente i risultati della valutazione del rischio (o quando vengono rilevati errori gravi)
- Registrazione e reporting
  - Registrare i risultati per l'uso futuro
  - Segnalare i risultati della valutazione del rischio



CONCLUSIONE

CONCLUSIONE

- La valutazione del rischio è una pratica importante per gestione della sicurezza di un sistema cyber

- La valutazione del rischio richiede:
  - Buona pianificazione
  - Tempo
  - Sforzo
  - Buona conoscenza del sistema cyber
  - Ottima conoscenza della sicurezza cyber
  - Esperienza nella gestione del rischio

- Ci sono altri modi per trattare i rischi
  - Non solo riduzione del rischio

DOMANDE?

This course is based on the knowledge obtained in the scope of the following EU projects:

SPARTA

MEDINA