Rischio, certificazione e governance

Massimo Carnevali

Massimo Carnevali
posta@massimocarnevali.com
https://it.linkedin.com/in/massimocarnevali

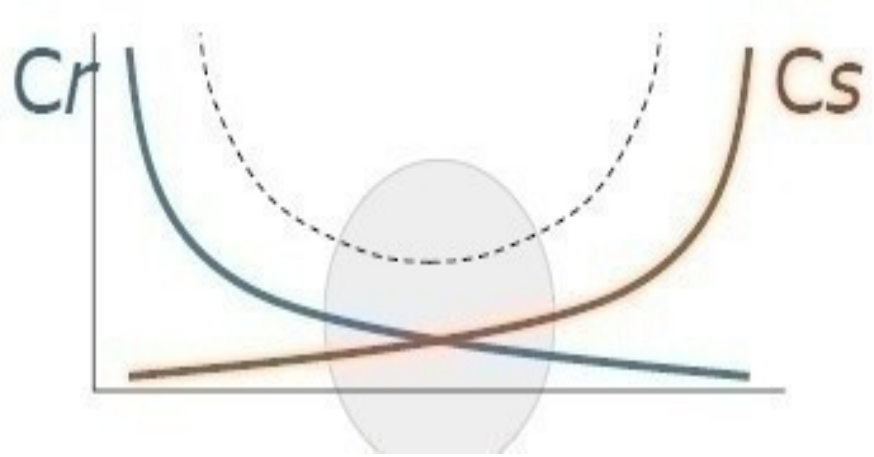
Rischio, certificazione e governance

- Analisi dei rischi e bilancio costi-benefici-semplicità
- Certificazioni
- Cenni di gestione dei processi IT in ottica di sicurezza
- Backup e dintorni

..

Rischi e bilancio costi-benefici-semplicità

Costi vs analisi dei rischi



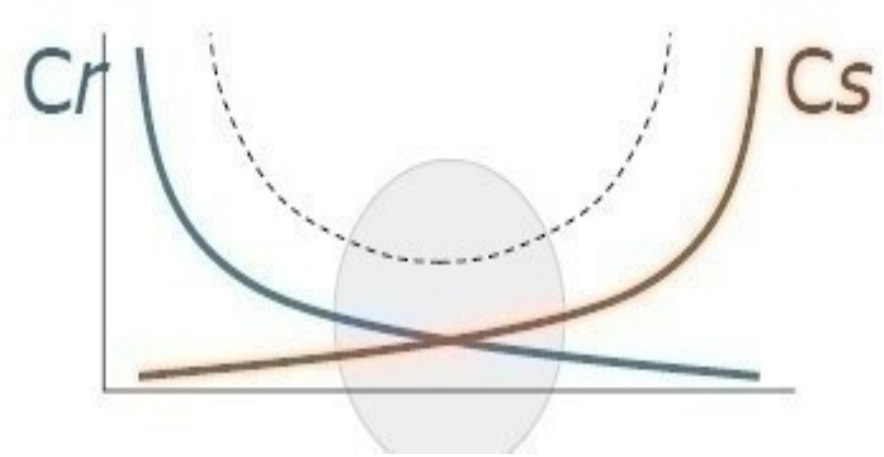
Nella definizione di un budget si esercita il tentativo di conciliare elementi contrastanti: il costo di un prodotto vs il beneficio previsto.

Nel caso di investimenti in sicurezza, come tutte le misure preventive, è spesso difficile quantificare il ritorno previsto; invece è più evidente come quantificare i costi. Si può cioè più facilmente ipotizzare un costo a cui si dovrebbe far fronte se non si adottano misure adeguate.

Disegnando qualitativamente le curve dei costi legati al rischio (Cr) e di quelli legati agli investimenti per la sicurezza (Cs), risulta evidente che il miglior compromesso è quello nell'intorno del minimo dei costi totali (linea tratteggiata=somma dei costi).

Rischi e bilancio costi-benefici-semplicità

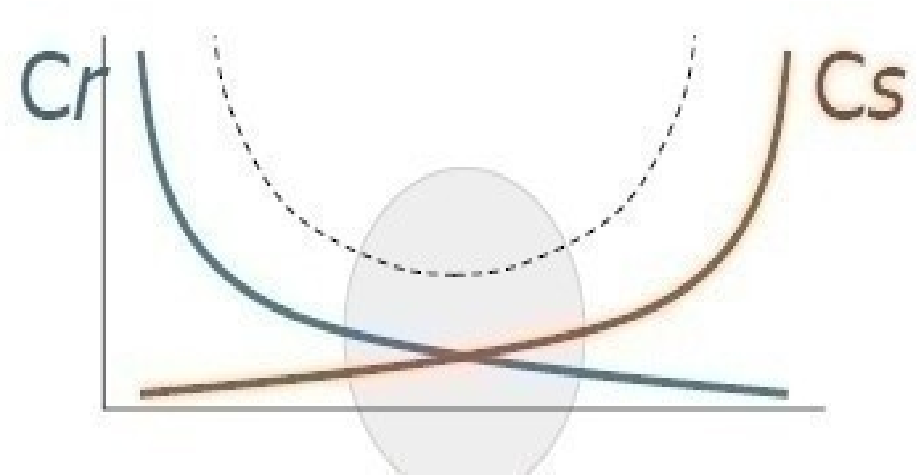
Modello Gordon-Loeb



https://en.wikipedia.org/wiki/Gordon%E2%80%93Loeb_model

Quindi quando dobbiamo spendere?
Quanto vale il punto minimo della curva?
Secondo il modello Gordon-Loeb il valore giusto è intorno al 37% del valore dei danni in caso di perdita dei dati
“More specifically, the model shows that it is generally uneconomical to invest in information security activities (including cybersecurity or computer security related activities) more than 37 percent of the expected loss that would occur from a security breach.”

Rischio residuo



Come si vede dal grafico (e come dice il buonsenso) rimane sempre una quota di rischio residuo.

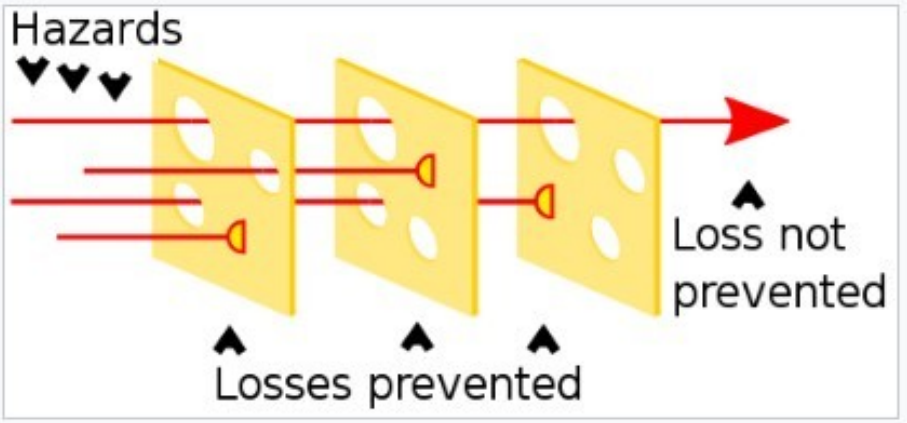
Tendenza recente: trasferimento del rischio residuo → assicurazione.

In Italia è un mercato in crescita, è già molto attivo negli USA.

Non solo trasferimento economico ma anche supporto nei momenti critici.

Ovviamente bisogna leggere le clausole in piccolo ...

Swiss cheese model



Il modello del formaggio svizzero (con i buchi). Ogni strumento di protezione riduce, ma non azzera, il rischio. Ognuno ha i suoi buchi ma se li uso assieme posso sperare che i buchi non coincidano e l'efficacia aumenti.

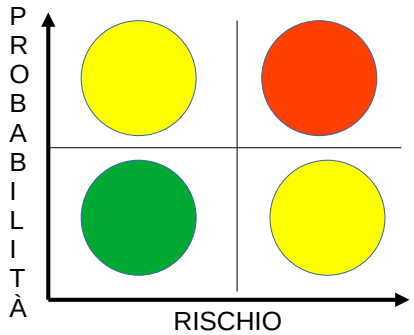
Non nasce dall'informatica ma dai modelli di rischio aeronautici e sanitari (ad esempio).

https://en.wikipedia.org/wiki/Swiss_cheese_model

Rischi e bilancio costi-benefici-semplicità

Modellare il rischio

- Dove sono più vulnerabile ad un attacco? (analisi flussi dati, superficie di attacco ecc.)
- Quali sono i rischi principali su questi punti esposti?
- Cosa debbo fare per proteggermi da questi attacchi?

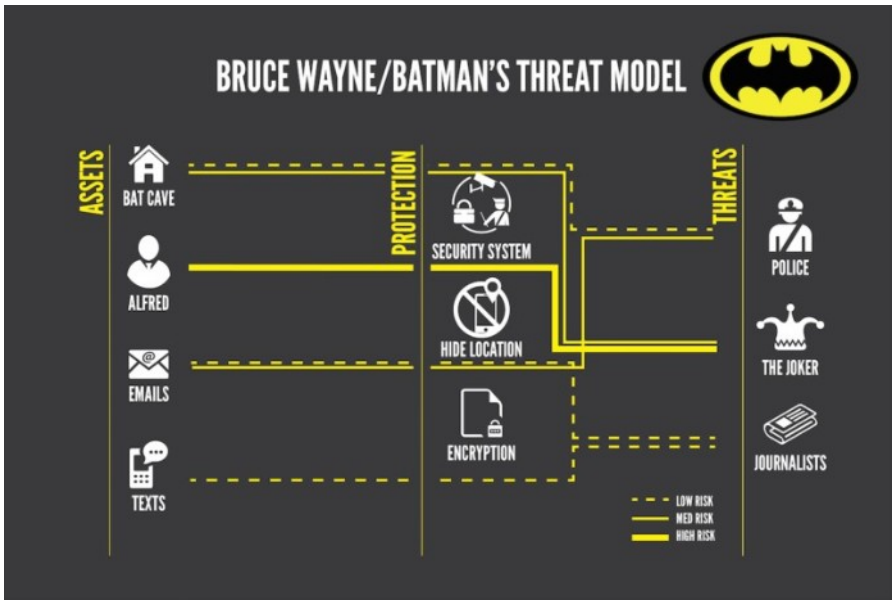


Sono ragionamenti che facciamo regolarmente nella nostra vita senza rendercene conto.

https://en.wikipedia.org/wiki/Threat_model
https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html

Rischi e bilancio costi-benefici-semplicità

Modellare il rischio

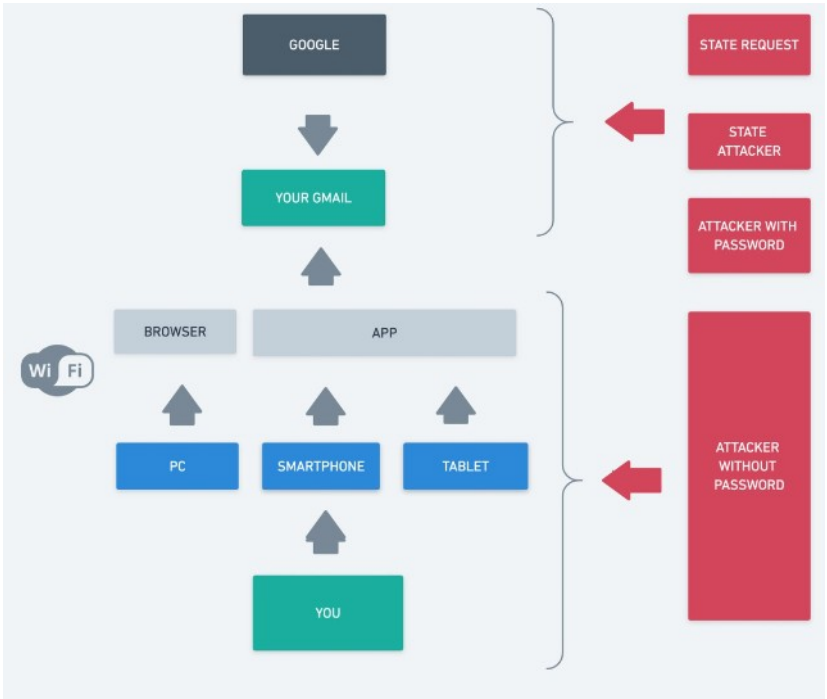


Identificare gli attaccanti, l'attaccabile e i sistemi di protezione.

Diversi modelli ICT (Stride, PASTA, TRIKE) e tools

https://arstechnica.com/information-technology/2017/07/how-i-learned-to-stop-worrying-mostly-and-love-my-threat-model/

Rischi e bilancio costi-benefici-semplicità



Farlo anche per la sicurezza informatica personale
https://guerredirete.substack.com/p/guerre-di-rete-facciamo-threat-modeling

Rischi e bilancio costi-benefici-semplicità

Sicurezza
=
Compromesso

Quindi la sicurezza non è un valore assoluto ma è un compromesso: “la spesa è commisurata al valore di ciò che sto assicurando?”

Ancora più complicato: “sto spendendo per essere al sicuro oppure per sentirmi sicuro?”

Facciamo continuamente scelte di questo tipo e l’evoluzione ci dice che dovrebbero sopravvivere quelli che le fanno giuste (ma non siamo tarati per le scelte del mondo presente).

Rischi e bilancio costi-benefici-semplicità

La percezione della sicurezza

Security is both a feeling and a reality, and they're not the same.

- Alternative A: A sure gain of $500.
- Alternative B: A 50% chance of gaining $1,000.

- Alternative C: A sure loss of $500.
- Alternative D: A 50% chance of losing $1,000.

84% A vs 16% B
70% D vs 30% C

The Psychology of Security - Bruce Schneier

https://www.schneier.com/essays/archives/2008/01/the_psychology_of_se.html

Rischio uguale in tutti e quattro i casi (guadagno o perdita statisticamente uguale).

https://www.ted.com/talks/bruce_schneier

Rischi e bilancio costi-benefici-semplicità

Percezione vs realtà:

- Spettacolare vs comune
- Ignoto vs famigliare
- Identificato vs anonimo
- Controllo della situazione
- Media

Che cosa influenza il rapporto percezione/realtà?

1) Rischi spettacolari vs comuni (aereo vs auto)
2) Sconosciuto vs famigliare (violenza alle donne)
3) Identificato vs anonimo (ISIS vs ubriaco)
4) Controllo della situazione (terrorista vs auto o sigaretta)
5) Influenza dei media (COVID-19)

Sono tutti temi che si applicano anche alla cyber security:

1) Mega attacchi vs perdita di dati
2) “I cattivi sono fuori” vs dipendente infedele
3) CIA/Russi/anonymous vs mille altri attaccanti
4) Cloud vs server in casa
5) CIO influenzati da quanto leggono sulla stampa indirizzano le spese

Rischi e bilancio costi-benefici-semplicità

Economia comportamentale

Teoria del prospetto

Decision #1:
A) 100% chance of receiving $3,000
B) 80% chance of receiving $4,000, 20% chance of receiving nothing

A expected outcome is $3,000 while B is $3,200 but 80% of subjects choose option A

Decision #2:
C) 100% chance of losing $3,000
D) 80% chance of losing $4,000, but a 20% chance of losing nothing

C expected outcome is losing $3,000 while D is losing $3,200. 92% of people choose D

https://en.wikipedia.org/wiki/Behavioral_economics
Economia comportamentale vs economia tradizionale: l'uomo reale non sempre sceglie la soluzione matematicamente migliore.
Teoria del prospetto: come scegliamo.
https://en.wikipedia.org/wiki/Prospect_theory
Non quella razionalmente più conveniente ma quella che ci fa soffrire meno.
L'attaccante opera nel dominio dei guadagni (A-B) mentre il difensore opera nel dominio delle perdite (C-D), questa asimmetria falsa le scelte strategiche.
Bisogna tenerne conto.

Rischi e bilancio costi-benefici-semplicità

Economia comportamentale

Due escursionisti stanno camminando in una foresta quando all'improvviso, un orso gigante salta fuori dal bosco. Uno degli escursionisti apre lo zaino e si mette le scarpe da corsa. Il suo amico lo guarda e dice:
"Cosa stai facendo? Sei pazzo? Non puoi correre più veloce dell'orso!"
"Lo so, tutto ciò che devo fare è correre più veloce di te!"

Morale

Magari non sei protetto al 100% ma se sei un bersaglio “costoso” da attaccare gli attaccanti puntano a chi è meno protetto di te.

Anche l’attaccante comunque ha dei costi e deve fare un’analisi costi-benefici. Se “vali” poco e sei costoso da attaccare magari attaccano qualcun altro.

- Quanto è disposto a investire l’attaccante? (soldi, tempo, risorse)
- Quanto valiamo noi per l’attaccante? (Quanto può chiedere di riscatto? Quanto valgono i dati che può esfiltrare? Quanto “contante” può rubarci?)
- Quale difesa rende l’attacco non conveniente? (Magari non è la migliore ma rende l’attacco molto più costoso) (esempio greylisting)

Economia comportamentale

Come decidiamo?

- Punto di riferimento
- Cerchiamo di evitare le perdite
- Non siamo lineari
- Poco sensibili ai grandi valori

- Cerchiamo un punto di riferimento e ragioniamo in base a quello (può essere diverso per attaccante e difensore, può muoversi a velocità diversa nei due casi)
- Cerchiamo di evitare le perdite (a parità di valore una perdita ci fa soffrire 2,25 volte più di quanto lo stesso guadagno ci faccia piacere)
- Non siamo lineari, sottovalutiamo le grandi probabilità e sopravvalutiamo quelle piccole (e preferiamo le certezze)
- Più lontano il guadagno o la perdita è dal punto di riferimento meno siamo precisi nei ragionamenti

Tutti fattori che influenzano le strategie di difesa: esempio 2 factor autentication, utenti amministratori dei PC ecc. sarebbero comodi ma non si usano.

Articolo sul tema:
https://medium.com/@kshortridge/behavioral-models-of-infosec-prospect-theory-c6bb49902768

Rischi e bilancio costi-benefici-semplicità

E poi guardiamo troppi (tele)film! (e ragioniamo poco)

I terroristi non guardano i film!
https://www.schneier.com/essays/archives/2005/09/terrorists_dont_do_m.html

Esempio di ragionamento fallace:

Se cerchi di salire in aereo con una pistola vieni fermato e identificato, magari finisci in blacklist o vieni arrestato, sicuro la seconda volta hai problemi.

Se hai una bottiglietta da 110cc te la tolgono. Punto. Puoi provarci tutti i giorni e non ne rimane traccia. Quindi puoi tentare all'infinito con una boccetta di esplosivo e prima o poi ci riuscirai.

Quindi ha senso togliere le bottigliette e basta?

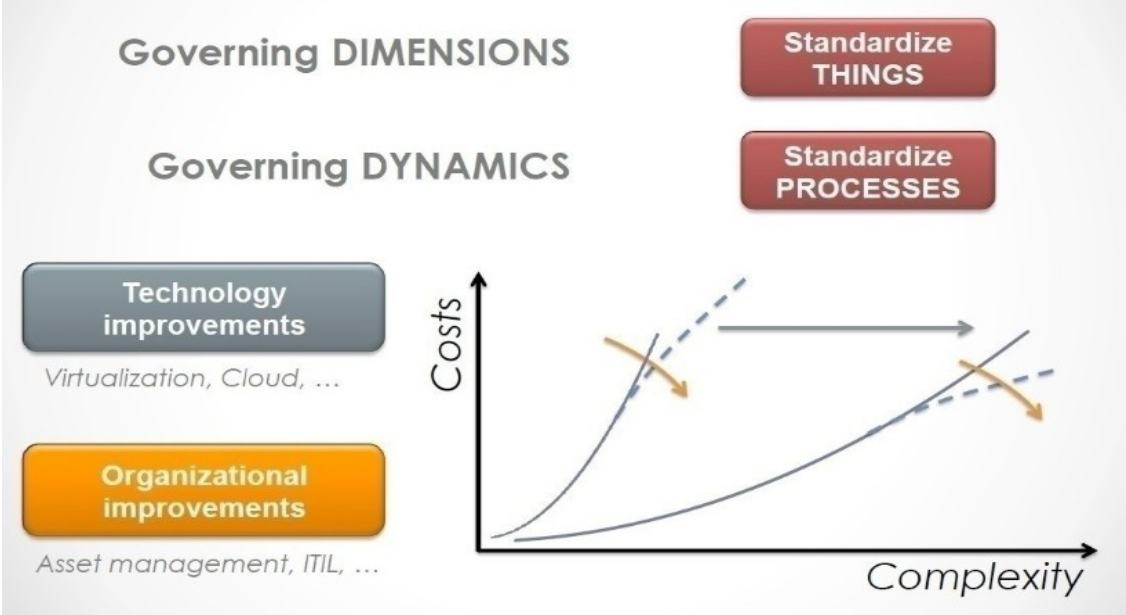
Di nuovo, non aumenta la sicurezza ma solo il senso di sicurezza.

Evoluzione e analisi della complessità

La complessità è nemica della sicurezza.
Per ridurre i rischi debbo ridurre anche la complessità.

Vi sono due dimensioni principali da percorrere per il raggiungimento del governo della complessità IT:
- la cardinalità dei fenomeni
- l'organizzazione del servizio.

Rischi e bilancio costi-benefici-semplicità



 18

Vi sono due dimensioni principali da percorrere per il raggiungimento del governo della complessità IT:

- la cardinalità dei fenomeni
- l'organizzazione del servizio.

Nella prima dimensione sfruttiamo la tecnologia per introdurre o accrescere la standardizzazione delle cose (ad esempio per ridurre il numero di modelli di computer impiegati: automatismi per l'installazione, virtualizzazione di server e client, ecc) e ottenere quindi una semplificazione nella gestione dell'installato.

Nella seconda sfruttiamo invece nuovi modelli o standard organizzativi, che consentono a gruppi di lavoro eterogenei e/o distribuiti di effettuare la gestione dell'installato

Rischi e bilancio costi-benefici-semplicità

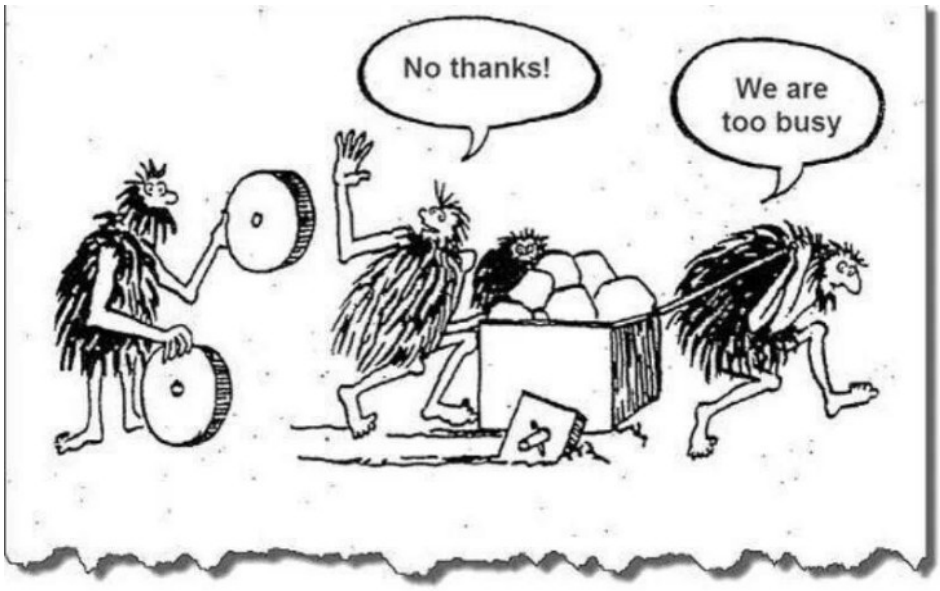
- Sicuro
- Economico
- Semplice

Rischi e bilancio costi-benefici-semplicità

- Sicuro
- Economico
- Semplice

Scegline due!

Rischi e bilancio costi-benefici-semplicità



Poi ovviamente c’è il problema di dover intervenire su ambienti “vivi”.

Certificazione ISO/27001

https://en.wikipedia.org/wiki/ISO/IEC_27001:2013

ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS) within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

Deve essere confermata ogni anno.

I controlli presenti nell'Annex A rappresentano un'ottima checklist per iniziare.

Parte di una famiglia di standard più ampia
https://en.wikipedia.org/wiki/ISO/IEC_27000-series

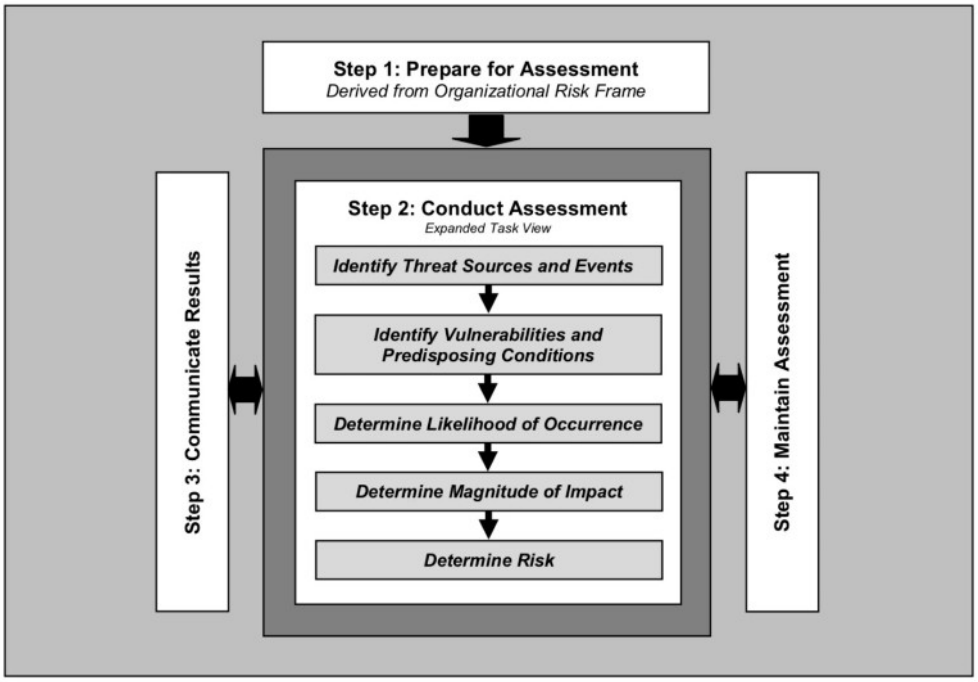
Certificazioni

NIST Framework

https://www.nist.gov/cyberframework
National Institute of Standards and Technology (NIST), agenzia USA per la promozione di innovazione e competitività.

The Framework is voluntary guidance, based on existing standards, guidelines, and practices, for critical infrastructure organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders.

Certificazioni



https://www.nist.gov/cyberframework
National Institute of Standards and Technology (NIST), agenzia USA per la promozione di innovazione e competitività.

NIST SP-800-30 Risk Assessment Process.

Certificazioni

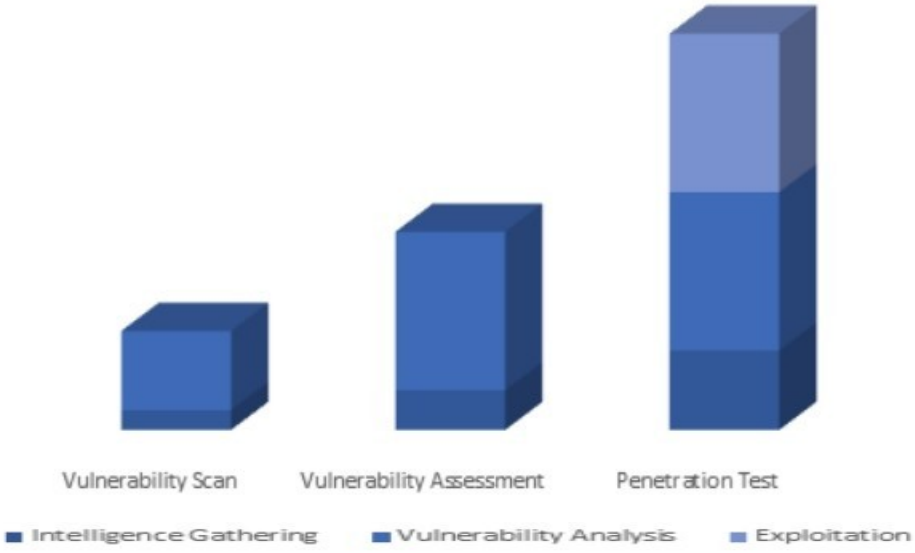
ISA/IEC 62443

(ex ISA99)
Per indirizzare i temi di information security in contesti come quello dell'automazione industriale.
ISA/IEC-62443 is a series of standards, technical reports, and related information that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS). This guidance applies to end-users (i.e. asset owner), system integrators, security practitioners, and control systems manufacturers responsible for manufacturing, designing, implementing, or managing industrial automation and control systems.

Questo e altri standard qui:
https://en.wikipedia.org/wiki/Cyber_security_standards

Certificazioni

Analisi preventive



Analisi preventive (audit)

- Scansione = raccolta di informazioni (automatico)
- Assessment = consolido i dati e verifico se ci sono falsi positivi (ad. es.) (semi automatico)
- Penetration test = provo a fare l'exploit delle vulnerabilità e ad entrare effettivamente nei sistemi (richiede operazioni manuali e conoscenza dei sistemi target)

Video interessanti di storie vere di pen-tester:
https://www.rapid7.com/info/under-the-hoodie/

Certificazioni

(U) Table 1. Security Weaknesses Identified at [redacted] Facilities Visited

Unclassified Security Weakness	Facility Visited*				
	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Multifactor Authentication Was Not Consistently Used	X		X		X
Network Vulnerabilities Were Not Consistently Mitigated	X	X			X
Server Racks Were Not Consistently Secured	X			X	
Data on Removable Media Was Not Consistently Protected and Monitored		X	X	X	
Intrusion Detection Was Not Implemented			X		
Administrators Did Not Require or Maintain Justification for Access	X	X	X	X	X
Physical Security Controls Were Not Implemented			X	X	X **Unclassified**

*(U) The [redacted] maintained separate facilities for administrative activities at the [redacted]. Therefore, checkmarks in those columns could indicate issues at either an administrative facility, a lab, or both. For details, see the discussion section of this report.

Source: The DoD OIG.

Esempio di output di audit.
In questo caso si tratta della verifica della sicurezza del sistema di controllo dei missili nucleari balistici degli Stati Uniti. :-O

https://www.zdnet.com/article/us-ballistic-missile-systems-have-very-poor-cyber-security/

Gestione e sicurezza

Gestione e sicurezza

Senza gestione non può esserci sicurezza.

Come faccio a definire delle policy di sicurezza aziendali se non conosco ruoli, funzioni, necessità ecc. degli utenti ?

Il perimetro aziendale a volte è complesso (partecipate, consociate, consulenti, insourcing, outsourcing ecc.).

Nessuna tecnologia può aiutarmi a sapere “chi fa che cosa” in azienda.

Serve organizzazione, metodo, policy e profonda conoscenza del proprio “environment”.

A volte bisogna comunque arrivare a soluzioni di compromesso.

Separazione delle funzioni

Ripensare organigrammi e funzioni in modo da separare le funzioni.
Evitare la presenza di conflitti di interesse e situazioni di controllore e controllato nella stessa linea gerarchica.
Classico esempio: chi implementa sicurezza diverso da chi la verifica.
Responsabile sicurezza riporto molto alto nella scala gerarchica (richiesto dal GDPR).
Più facile utilizzando servizi in outsourcing (esternalizzati).

Gestione dei processi IT

Questo è complicato da mettere in sicurezza.

Gestione dei processi IT

Questo è più facile da mettere in sicurezza.

Enterprise backup

http://en.wikipedia.org/wiki/Backup

Salvataggio strutturato dei dati/sistemi/macchine critici per l'azienda seguendo precise policy.

Può servire per:

- Proteggere i dati da un incidente (rottura dischi, attacco informatico ecc.)
- Consentire il ripristino di situazioni stabili precedenti (recupero di file cancellati o modificati per errore, ricostruzione di una situazione al momento X, ripristino di un sistema allo stato precedente una modifica ecc.)

Non è difficile fare i backup … il difficile è fare il restore che ci interessa !

Backup=salvataggio di dati dinamici, concetto di retention

Archive=archiviazione di copia statica e perenne.

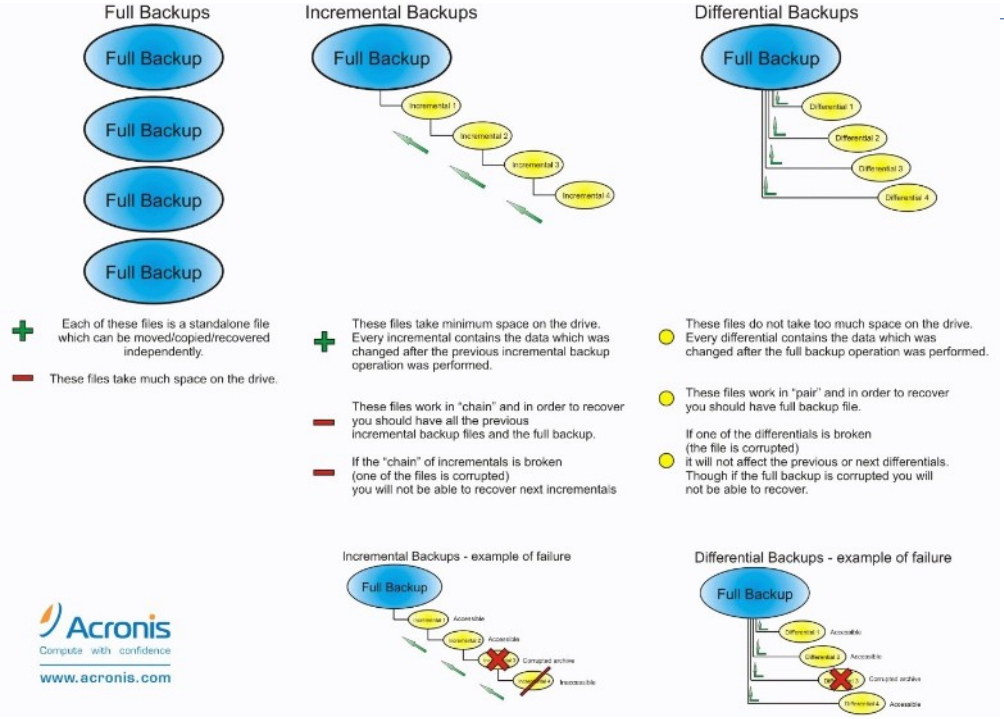
Enterprise backup

NB: Non è difficile fare i backup … il difficile è fare il restore che ci interessa!

http://en.wikipedia.org/wiki/Backup
Esempi di policy sono:

- Si effettua il backup notturno di tutti i sistemi server (non i client) e si tengono 2 copie di ciascun file; un file cancellato viene tenuto dal sistema per 60gg; settimanalmente si effettua una duplicazione dei nastri che viene trasportata e conservata in altro sito
- I database sono esportati su file ogni notte, il dump viene archiviato su nastro e l'archivio mantenuto per 15gg, cancellando a rotazione il più vecchio
- Di ogni sistema virtuale viene effettuato l'image backup differenziale ogni notte e consolidato ogni week-end; dall'insieme delle immagini differenziali accumulate durante la settimana si possono effettuare le procedure di restore

Backup e dintorni

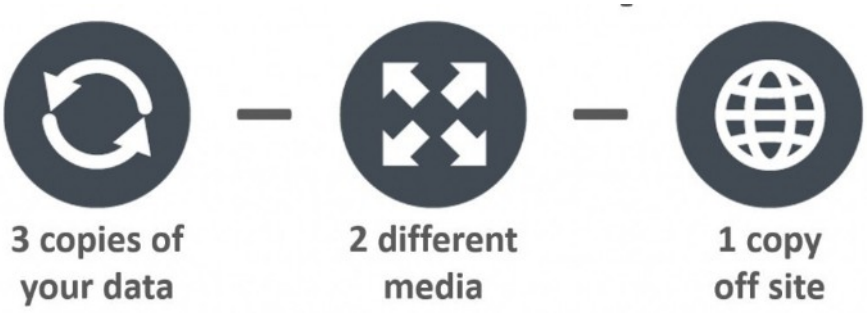


Backup full = salvo tutto tutte le volte

Backup incrementale = salvo quello che è cambiato dall'ultimo backup full oppure dall'ultimo incrementale

Backup differenziale = salvo quello che è cambiato dall'ultimo backup full

Backup 3-2-1



Regola del 3-2-1

Avere sempre almeno 3 copie dei propri dati: l'originale + due copie di riserva

Le copie debbono essere su almeno due media diversi (disco, nastro, CD, NAS, cloud ecc.)

Almeno una copia deve essere in un posto fisicamente distinto da quello dei dati originali (oppure nel cloud).

Business Continuity
Disaster Recovery

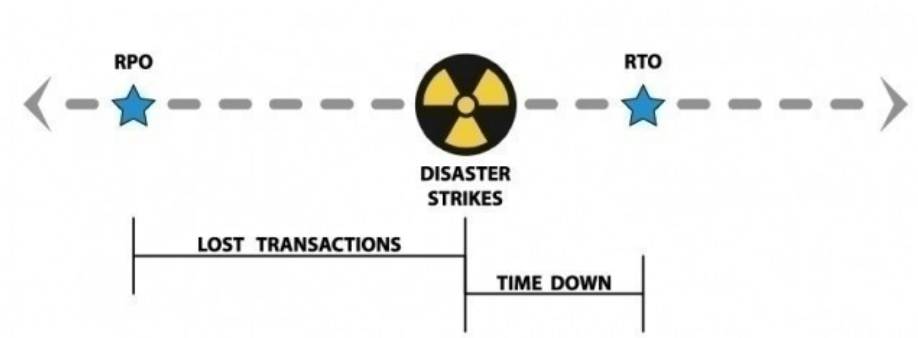
http://en.wikipedia.org/wiki/Business_continuity
http://en.wikipedia.org/wiki/Disaster_recovery

La Business Continuity non è un problema IT !

A che cosa serve infatti poter ripristinare tutte le risorse informatiche di supporto alla produzione e alla vendita se non si riescono a ripristinare le risorse primarie necessarie per svolgere queste funzioni (es. logistica, magazzino, linea di produzione)?

Per Disaster Recovery si intende normalmente il ripristino della struttura aziendale IT a fronte di un “disastro”. E' un “di cui” della Business Continuity.

RPO e RTO



RPO e RTO

Sono i parametri con cui si definiscono le performance di un sistema di backup adibito al Disaster Recovery: si riferiscono entrambi all'istante in cui avviene l'evento disastroso (perdita del sistema protetto).

Recovery Point Objective: tempo fra l'ultimo stato del sistema disponibile in una copia di backup e il momento del disastro.

Recovery Time Objective: tempo fra il momento del disastro e quello in cui il sistema alternativo comincia a essere disponibile

Sarebbe bello che fossero molto bassi ma, ovviamente, ha un costo.

Piano di Disaster Recovery

Disaster Recovery Site

L’elemento più importante di un progetto di Disaster Recovery non è tecnologico: Piano di Disaster Recovery.

Contiene la descrizione del sito di DR, le procedure necessarie per riattivare i sistemi remoti, indicando i responsabili di queste attività e i contatti delle ditte esterne da attivare (es. ISP).

Il piano di DR va mantenuto aggiornato con esplicite procedure di simulazione e test, tipicamente annuali.

Disaster Recovery Site

E’ un centro servizi remoto, dotato di sistemi, applicazioni e dati sufficienti e sufficientemente aggiornati per consentire a un’organizzazione di ripartire con le funzioni IT vitali in caso di grave disastro o indisponibilità prolungata nel tempo dei suoi sistemi principali

Esistono indicazioni sulla distanza fisica dal centro vitale IT.

Si stanno diffondendo soluzioni in cloud.

Backup e dintorni

.....

Ridondanze

Le caratteristiche di ridondanza costruttiva e di impiego dei dispositivi aumentano la sicurezza e la disponibilità dell'informazione:

- Doppia alimentazione
- Doppio allacciamento (su linee generali separate)
- Ventilazione ridondante (come numero di ventole e come controllo: sensori ecc)
- Alimentatori e ventole rimpiazzabili a caldo
- Data plane e Control plane separati (un fermo sul secondo non impedisce al dispositivo di funzionare almeno parzialmente)
- Hot/cold standby
- Ridondanza virtuale/reale
- Copie multiple dei dati
- Processi ridondati
- Data center replicati

Attenzione alle false ridondanze (es. rete mesh internet su singolo provider)

Backup e dintorni

Current infrastructures focus on BC / DR
- Backups
- Snapshots
- Replication

Add a focus on Cyber Resiliency
- Isolation
- Immutability
- Granularity

 41

Il concetto di resilienza informatica sta diventando vitale, occorre introdurre concetti quali: **isolamento, immutabilita', granularita'**.

L'isolamento può essere una separazione logica o fisica. "Air Gap" rappresenta un esempio di separazione. In generale, maggiore è la separazione, maggiore è la protezione, ma più tempo ci vuole per tornare in funzione,

L'immutabilità è in gran parte definita da quanto sia facile danneggiare o distruggere i dati.

La granularità si riferisce alla quantità di perdita di dati e alla quantità di tempo di inattività che la tua azienda può permettersi. Quanti dati può perdere la tua azienda senza impatto sui clienti?