ISACA®

Sistemi informativi: averne fiducia e trarne valore

Rome Chapter

Infrastruttura o applicazione
Ad ognuno la sua risk analysis

Ing. Marcello Mistre

Roma 30/09/2019

Agenda

- Presentazione relatore
- Considerazioni iniziali
- Analisi e gestione del rischio in ambito infrastrutturale
- Analisi e gestione del rischio in ambito applicativo
- Q&A

Agenda

- Presentazione relatore
- Considerazioni iniziali
- Analisi e gestione del rischio in ambito infrastrutturale
- Analisi e gestione del rischio in ambito applicativo
- Q&A

Presentazione relatore

Ing. Marcello Mistre

CISA, CISM, CGEIT, Lead Auditor ISO27001:2013

ISACAROMA – Membership Director

m.mistre@isacaroma.it

Agenda

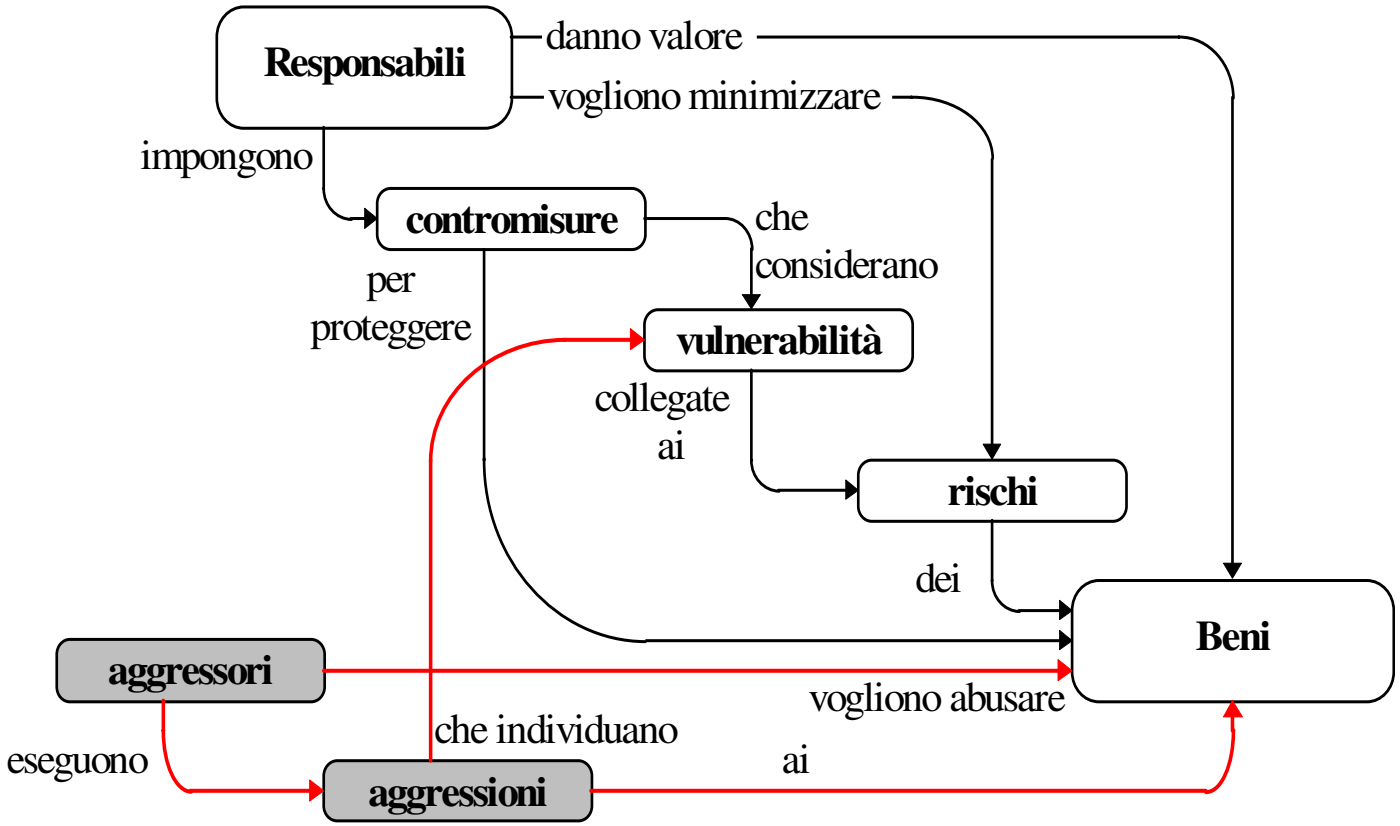
- Presentazione relatore
- Considerazioni iniziali
- Analisi e gestione del rischio in ambito infrastrutturale
- Analisi e gestione del rischio in ambito applicativo
- Q&A

Considerazioni iniziali

UN PO' DI NOMENCLATURA

- VULNERABILITA'
- MINACCIA
- PROBABILITA'
- IMPATTO
- RISCHIO

Considerazioni iniziali



Considerazioni iniziali

TIPI DI APPROCCIO

ANALISI QUANTITATIVA

ANALISI SEMI QUANTITATIVA

ANALISI QUALITATIVA

Considerazioni iniziali

QUANDO CI FERMIAMO?

?

Considerazioni iniziali

LIMITI DI UN'ANALISI QUANTITATIVA

Se il rischio è dato dal "prodotto" della probabilità per l'impatto:

Per la probabilità quasi sempre non esistono serie storiche che consentano l'applicazione di algoritmi probabilistici

Per l'impatto, le considerazioni sono quasi sempre soggettive, ottenute intervistando l'owner del bene di cui si sta valutando il rischio

Considerazioni iniziali

CORRELAZIONE TRA RISCHIO E CONTROMISURE

L'obiettivo dell'analisi e gestione del rischio è introdurre contromisure che limitino il rischio a un livello accettabile

Dato un rischio e una contromisura come si fa a determinare il valore (numerico) del rischio prima dell'applicazione della contromisura e dopo?

Come faccio a sapere di quanto si abbassa il rischio?

Così come non esiste il rischiometro, non esiste (tranne casi particolari) il contromisurometro!

Considerazioni iniziali

COSA VOGLIAMO PROTEGGERE?

Se l'ambito di applicazione è una infrastruttura, ad esempio un ced:

Si devono individuare le contromisure necessarie per ridurre i rischi gravanti sugli asset aziendali

Se l'ambito è di tipo applicativo:

Si devono individuare le contromisure necessarie per ridurre i rischi gravanti sui dati gestiti dall'applicazione

Considerazioni iniziali

SI NOTI CHE

Per una infrastruttura è impossibile parlare di dati:

I dati sono presenti tutti

In genere non si sa dove sono fisicamente residenti

Per una applicazione informatica:

Non ha senso parlare di asset (dipendono dall'ambiente in cui verrà installata)

Considerazioni iniziali

E’ errato utilizzare una metodologia unica per analizzare e gestire il rischio di una infrastruttura e di una applicazione

E’ NECESSARIO UTILIZZARE METODOLOGIE DIVERSE

Considerazioni iniziali

Nel seguito del seminario vedremo due modi diversi di affrontare il problema, applicando metodologie diverse nel caso dell'analisi di una infrastruttura e nel caso dell'analisi di una applicazione

Agenda

- Presentazione relatore
- Considerazioni iniziali
- Analisi e gestione del rischio in ambito infrastrutturale
- Analisi e gestione del rischio in ambito applicativo
- Q&A

Analisi e gestione del rischio in ambito infrastrutturale

Il processo di esplica in tre fasi:

- Asset inventory
- Analisi del rischio
- Gestione del rischio

Analisi e gestione del rischio in ambito infrastrutturale

Asset inventory

L'obiettivo finale è la protezione degli asset……

ma quali sono gli asset?

Gli asset sono:

- L'hardware
- Il software (ad eccezione del sw applicativo)
- I beni informativi

Analisi e gestione del rischio in ambito infrastrutturale

Asset inventory

I beni informativi sono tutti quegli asset che sono indispensabili per il funzionamento dei processi di business

Come fare per ricavare l'elenco dei beni informativi?

Si deve necessariamente partire dai processi di business, che quindi devono essere censiti

Se operiamo in un contesto in cui è in vigore una certificazione ISO9000 siamo avvantaggiati perchè i processi di business sono già censiti

Analisi e gestione del rischio in ambito infrastrutturale

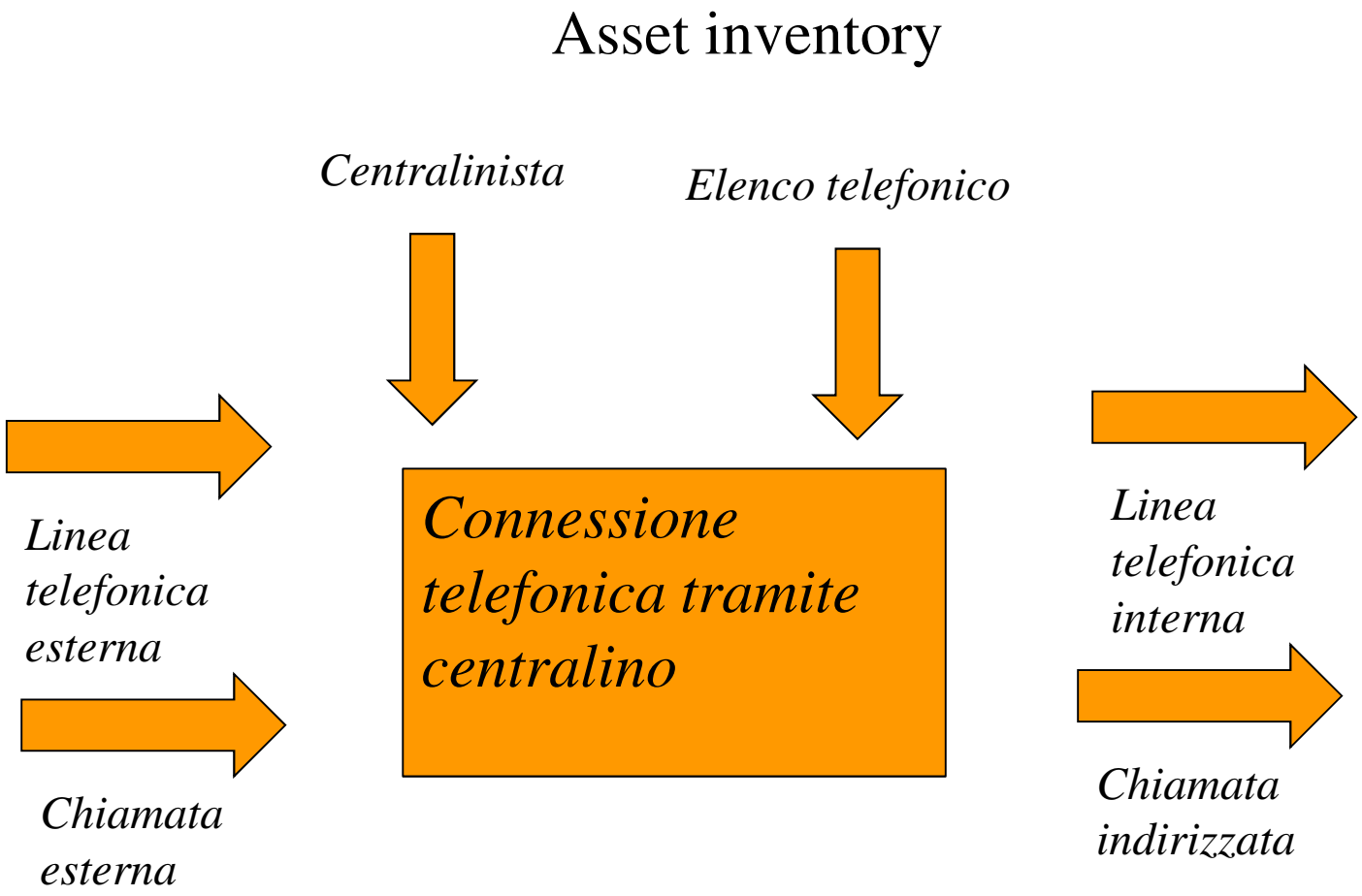
Asset inventory

Una volta censiti o ricavati i processi di business, si dovranno analizzare.

Possiamo ad esempio disegnare per ogni processo un diagramma IPO, facendo attenzione non solo agli input e agli output, ma anche ai controlli relativi al processo

Vediamo un esempio

Analisi e gestione del rischio in ambito infrastrutturale



Analisi e gestione del rischio in ambito infrastrutturale

Asset inventory

Con i risultati dell'analisi potrà essere redatto un documento riportante i beni hardware, i beni software e i beni informativi

Per una maggiore chiarezza i capitoli potranno essere poi suddivisi in paragrafi

Analisi e gestione del rischio in ambito infrastrutturale

Asset inventory

Struttura Hardware

Cablaggi

.....

.....

Elaboratori

.....

.....

Switches

.....

.....

Sottosistemi disco

.....

.....

Sottosistemi a nastri

.....

.....

Sottosistemi stampanti

.....

.....

Analisi e gestione del rischio in ambito infrastrutturale

Asset inventory

Struttura Software

Sistema Operativo

.....

Con i seguenti prodotti a corredo:

.....

.....

Data Communication

.....

.....

Data Base System & Administration

.....

.....

Prodotti forniti dal cliente

.....

.....

Asset inventory

Beni Informativi

Beni Informativi di Input

.....

.....

Beni Informativi di Output

.....

.....

Beni informativi di controllo

.....

.....

Analisi e gestione del rischio in ambito infrastrutturale

Asset inventory

Oltre alle tre categorie di asset se ne deve aggiungere una quarta, non meno importante.

IL PERSONALE

Come gli altri asset, anche la componente "personale" sarà soggetta alla risk analysis e anche per essa sarà individuata una serie di contromisure atte a ridurre il rischio per renderlo compatibile con gli obiettivi di sicurezza

Si suddividerà il personale tra:

- Personale interno
- Personale esterno

Analisi del rischio

Il passo successivo è quello di effettuare l'analisi dei rischi che gravano sugli asset individuati

Se il rischio è dato da probabilità per impatto, devono essere definite delle metriche per la probabilità e per l'impatto

Analisi del rischio

Esempio di classificazione della probabilità di accadimento di un evento

VALORE	CRITERIO
N	L'evento non risulta essersi mai verificato e/o ne appare estremamente improbabile il verificarsi nel futuro
B	L'evento non risulta essersi mai verificato ma si ritiene possibile che si verifichi in futuro
M	L'evento può essersi verificato in passato e comunque se ne ritiene probabile il verificarsi nel futuro
A	L'evento è percepito come frequente e facile ad accadere

Analisi del rischio

Esempio di classificazione dell'impatto di un evento

VALORE	CRITERIO
N	L'evento non comporta alcuna conseguenza
B	L'evento comporta una moderata compromissione delle caratteristiche RID dell'asset Le attività di business proseguono, presumibilmente con alcune difficoltà. Il ripristino delle caratteristiche RID dell'asset non comporta particolari difficoltà né costi elevati, e non impatta in maniera significativa sulle attività di business.

Analisi e gestione del rischio in ambito infrastrutturale

Analisi del rischio

Esempio di classificazione dell'impatto di un evento

VALORE	CRITERIO
M	L'evento comporta una compromissione significativa delle caratteristiche RID dell'asset. Le attività di business sono compromesse, con conseguenze percettibili a livello dell'intera azienda. Il ripristino delle caratteristiche RID dell'asset richiede attività dispendiose in termine di tempo e/o costo e può sottrarre risorse in modo significativo dai processi di business.
A	L'evento comporta una compromissione grave o irrimediabile delle caratteristiche RID dell'asset. Le attività di business si interrompono, con gravi conseguenze a livello aziendale. Il ripristino delle caratteristiche RID dell'asset può non essere possibile del tutto, ovvero richiedere rilevanti impegni di risorse, tempi e costi.

Analisi del rischio

Valutazione del rischio dalla combinazione dei valori di probabilità e impatto

	N	B	M	A
N	N	N	N	N
B	N	B	M	M
M	N	M	M	A
A	N	M	A	A

Analisi del rischio

Per una migliore trattazione è opportuno considerare l'impatto (e quindi il rischio) per ciascun elemento della terna RID:

- Riservatezza
- Integrità
- Disponibilità

Analisi e gestione del rischio in ambito infrastrutturale

Analisi del rischio

Per ogni asset definito nell'asset inventory si espliciteranno:

- Vulnerabilità
- Minacce relative a ciascuna vulnerabilità individuata
- Valutazione della probabilità della minaccia
- Valutazione dell'impatto della minaccia (terna RID)
- Valutazione del rischio (terna RID)

Analisi e gestione del rischio in ambito infrastrutturale

Asset	Vulnerabilità	Minaccia	Probab	Impatto			Rischio		
				R	I	D	R	I	D
Cavi di rete	Accessibilità	Manomissione dei cablaggi dati	B	B	N	M	B	N	M
		Intercettazione delle comunicazioni	B	M	N	N	M	N	N
		Interruzione dei collegamenti dati	B	N	N	M	N	N	M
	Soggetti a rottura	Rottura cavi o connettori	A	N	N	M	N	N	A

Analisi del rischio

QUICK WINS

Quando si individua un rischio alto per almeno un elemento della terna RID è opportuno fornire subito delle indicazioni per la mitigazione, prima ancora di produrre il piano di gestione del rischio.

Analisi del rischio

QUICK WINS

V1	Asset	Cavi di rete		
Vulnerabilità	Soggetti a rottura			
Descrizione Il grado di minaccia elevato dipende dalla presenza rilevata in passato di ratti nei cavedi della sala macchine. Il rischio è che la frequenza di rottura dovuta a tale causa sia elevata.				
Possibili Minacce		Rischio		
		R	I	D
Rottura cavi o connettori		N	N	A
Contromisure	Misure di sicurezza fisica Frequenti derattizzazioni dei locali, compresi sottopavimenti e cavedi. Frequenti ispezioni dei cavi.			

Analisi e gestione del rischio in ambito infrastrutturale

Analisi del rischio

REQUISITI COGENTI

Sono i requisiti che devono essere applicati a fronte di:

- Leggi nazionali o europee
- Regolamentazioni di settore (es PSD2)
- Standard volontari (es ISO27001)

Analisi e gestione del rischio in ambito infrastrutturale

Analisi del rischio

REQUISITI COGENTI

E’ opportuno censire nell’analisi del rischio leggi, regolamenti e standard applicabili, e per ciascuno determinare i controlli e a quali asset si applicano

Analisi del rischio

REQUISITI COGENTI

Requisito	Controllo	Asset
Provvedimento del Garante Privacy del 27/11/08 (GU 300/08)	Applicazione delle misure tecniche sui log	Z/OS v.2.1
	Nomina degli amministratori	Personale interno
		Personale esterno

Analisi del rischio

Come si fa a determinare vulnerabilità e minacce che gravano sugli asset?

- Logica
- Esperienza
- Supporto di esperti

Analisi del rischio

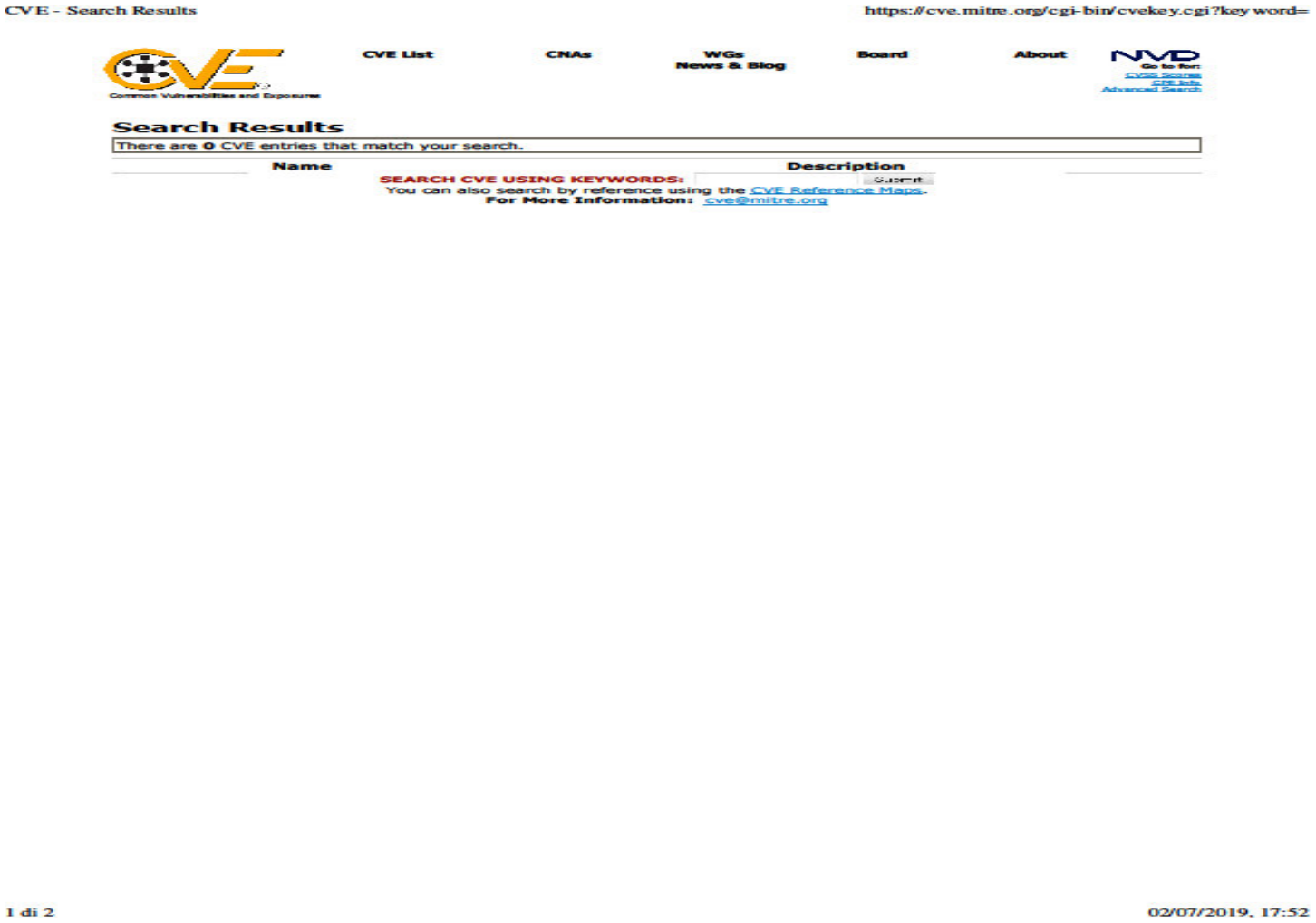
Per le componenti infrastrutturali si può ricorrere a una serie di database.

I più noti sono:

- MITRE (https://cve.mitre.org/)
- NVD NIST (https://nvd.nist.gov/vuln/search)

Analisi e gestione del rischio in ambito infrastrutturale

Analisi del rischio


CVE - Search Results

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=

CVE List CNAs WGs News & Blog Board About NVD

Search Results

There are 0 CVE entries that match your search.

Name Description

SEARCH CVE USING KEYWORDS: Submit

You can also search by reference using the CVE Reference Maps.

For More Information: cve@mitre.org

1 di 2

02/07/2019, 17:52

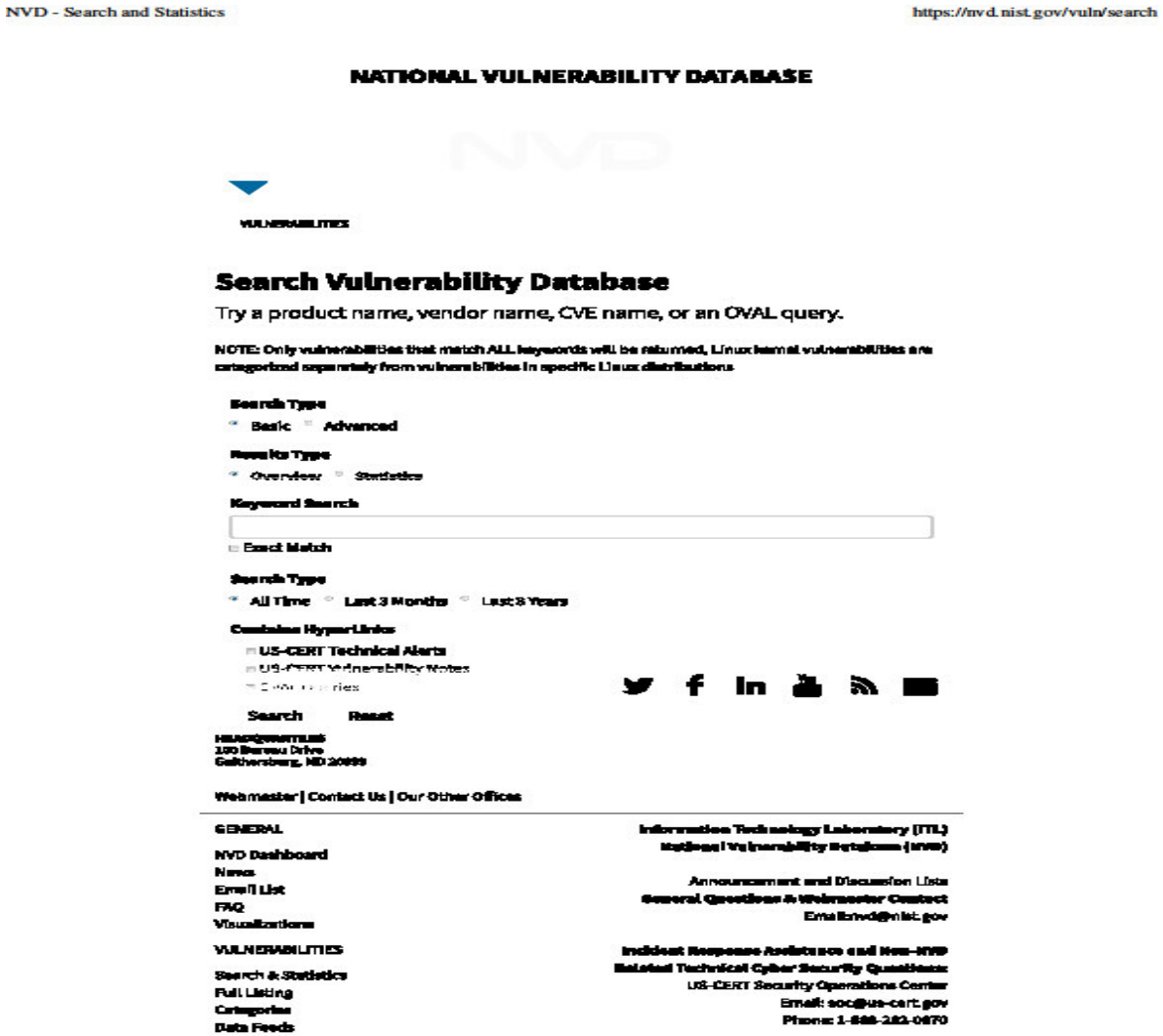
Analisi e gestione del rischio in ambito infrastrutturale

Analisi del rischio

Asset	Vulnerabilità	Minaccia	Probab	Impatto			Rischio		
				R	I	D	R	I	D
Microsoft SQL Server 2005 SP3 / 2008 R2	Collegabile in rete	Denial of Service Es: CVE-2014-4061	B	N	N	A	N	N	M
		Esecuzione di codice arbitrario Es:CVE-2012-2552	B	M	M	A	M	M	M
		Acquisizione di privilegi Es: CVE-2015-1761	B	M	B	A	M	B	M

Analisi e gestione del rischio in ambito infrastrutturale

Analisi del rischio



NVD - Search and Statistics https://nvd.nist.gov/vuln/search

NATIONAL VULNERABILITY DATABASE

VULNERABILITIES

Search Vulnerability Database

Try a product name, vendor name, CVE name, or an OVAL query.

NOTE: Only vulnerabilities that match ALL keywords will be returned. Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions

Search Type
Basic Advanced

Results Type
Overview Statistics

Keyword Search
Exact Match

Search Type
All Time Last 3 Months Last 3 Years

Contains Hyperlinks
US-CERT Technical Alerts
US-CERT Vulnerability Notes
OVAL queries

Search Reset

100 Bureau Drive
Gaithersburg, MD 20899

Webmaster | Contact Us | Our Other Offices

GENERAL
NVD Dashboard
News
Email List
FAQ
Visualizations

VULNERABILITIES
Search & Statistics
Full Listing
Categories
Data Feeds

Information Technology Laboratory (ITL)
National Vulnerability Database (NVD)

Announcement and Discussion Lists
General Questions & Webmaster Contact
Email: nvd@nist.gov

Incident Response Assistance and Non-NVD
Related Technical Cyber Security Questions:
US-CERT Security Operations Center
Email: soc@us-cert.gov
Phone: 1-888-282-0870

1 di 2 02/07/2019, 17:57

Analisi e gestione del rischio in ambito infrastrutturale

Gestione del rischio

Occorre innanzi tutto stabilire un criterio per il rischio accettabile

Considerando che come abbiamo visto nella maggior parte dei casi non esiste un rischiometro e un contromisurometro, anche il criterio di definizione del rischio accettabile sarà di tipo qualitativo

Gestione del rischio

Un esempio di rischio accettabile potrebbe essere il seguente

Viene definito accettabile un rischio di livello nullo o basso su tutte le componenti della terna RID, oppure medio su almeno una delle componenti della terna RID purchè mitigato da almeno una contromisura, oppure alto su almeno una delle componenti della terna RID purchè mitigato da due o più contromisure

Gestione del rischio

Compito della gestione del rischio è quindi quella di definire una serie di contromisure ed applicarle ai rischi individuati al fine di ricondurli ad un livello ritenuto accettabile

E' consigliabile suddividere il documento in due parti.

La prima riporterà l'elenco delle contromisure, suddivise per:

- beni hardware
- beni software
- beni informativi, attività di servizio e personale

Gestione del rischio

Per ogni contromisura verrà indicato:

- codice
- titolo
- collegamento con annex A ISO27001 (opzionale)
- descrizione
- modalità di implementazione
- stato dell'implementazione

Analisi e gestione del rischio in ambito infrastrutturale

Gestione del rischio

Nella seconda parte del documento verrà riportato per ogni asset il risultato dell'analisi del rischio, omettendo vulnerabilità, probabilità e impatto e riportando il rischio per le componenti della terna RID ed i codici delle contromisure che si applicano al rischio

Se il rischio accettabile è quello visto prima, potranno omettersi gli asset che hanno tutti rischi nulli o bassi e le minacce di ogni asset che hanno rischio basso o nullo per tutte le componenti della terna RID

Gestione del rischio

CAVI DI RETE

Minaccia	Rischio			Contromisure
	R	I	D	
Manomissione dei cablaggi dati	B	N	M	H01
Intercettazione delle comunicazioni	M	N	N	H01
Interruzione dei collegamenti dati	N	N	M	H01;H02;H16; H17
Rottura cavi o connettori	N	N	A	H01;H02;H17

Gestione del rischio

H01: Protezione fisica dei cablaggi (rif. 9.2.3)

Descrizione: *I cavi e le connessioni di trasporto dati devono essere fisicamente protette; cablaggi elettrici e cablaggi dati devono essere fisicamente separati*

Modalità di implementazione: *Ove possibile i cavi di trasmissione dati devono essere contenuti all'interno di canalizzazioni, cavedii, e armadi di derivazione fisicamente inaccessibili a chiunque tranne agli addetti alla posa e manutenzione dei cavi stessi.*
I cablaggi elettrici devono essere protetti da apposite canalizzazioni a norme CEI

Piano di implementazione: *Attuato*

Gestione del rischio

H02: Manutenzione dei cablaggi (rif. 9.2.4)

Descrizione: *La rete elettrica e la rete dati devono essere periodicamente ispezionati e tempestivamente ripristinati in caso di danneggiamento*

Modalità di implementazione: *L'efficienza degli apparati di protezione elettrica viene verificata con cadenza semestrale/annuale dall'impresa di manutenzione; gli impianti di terra e di protezione contro le scariche atmosferiche, oltre ad essere sottoposti a controllo come anzidetto, con cadenza biennale sono verificati anche da apposti Organismi Notificati abilitati dal Ministero delle Attività Produttive (DPR 462/01). Le evidenze vengono segnalate con appositi report, per la successiva programmazione degli eventuali interventi correttivi.*

Piano di implementazione: *Attuato*

Gestione del rischio

H16: connettività di back-up (rif. 10.3.1)

Descrizione: *Predisposizione di una connessione alternativa in caso di interruzione della connessione principale*

Modalità di implementazione: *Presenza di un piano di disaster recovery che garantisca la continuità dei servizi prestati in caso di interruzione della connessione principale.*

Piano di implementazione: *Attuato*

Gestione del rischio

H17: derattizzazione dei locali (rif. 9.2.2, 10.6.1)

Descrizione: *Attuazione di derattizzazione dei locali, compresi sottopavimenti e cavedii.*

Modalità di implementazione: *le attività di derattizzazione sono previste nel contratto in essere con xxxxxxxx. Le infrastrutture di connessione sono comunque dotate di cavi di collegamento antiratto, realizzati con adeguata schermatura, per la protezione di eventuali danni provocati dai ratti.*

Piano di implementazione: *Attuato*

Analisi e gestione del rischio in ambito infrastrutturale

Gestione del rischio

C'è ancora una cosa da fare: considerare i requisiti cogenti

Nell'analisi del rischio si erano individuate leggi, regolamenti e standard applicabili, e per ciascuno si erano determinati i controlli e a quali asset si devono applicare

Nel documento di gestione del rischio, nella seconda parte (risultanze dell'analisi del rischio) per ogni asset si dovranno riportare, ove applicabili, i requisiti cogenti, il controllo e il codice delle contromisure (che verranno dettagliate nella prima parte del documento)

Analisi e gestione del rischio in ambito infrastrutturale

Gestione del rischio

ASSET XXX

Requisito	Controllo	Contromisure
Provvedimento del Garante Privacy del 27/11/08 (GU 300/08)	Applicazione delle misure tecniche sui log	S03

Gestione del rischio

PERSONALE INTERNO

Requisito	Controllo	Contromisure
Provvedimento del Garante Privacy del 27/11/08	Nomina degli amministratori	B26

Gestione del rischio

S03: Registrazione audit (rif. 15.1.4, 15.3.1)

Descrizione:*registrazione delle attività compiute sul sistema*

Modalità di implementazione: *il controllo delle attività svolte sul sistema si avvale dei log di sistema ottenuti tramite SMF; tale log soddisfa anche i requisiti di logging delle attività degli amministratori di sistema richiesti dal provvedimento del Garante della privacy del 27/11/2008.*

Piano di implementazione: *Attuato*

Gestione del rischio

B26: Nomina incaricati e amministratori di sistema (rif. 15.1.1, 15.1.4)

Descrizione:*Attuazione degli adempimenti in materia di nomina di incaricati al trattamento e di amministratori di sistema ai sensi della legge 196/03 e del provvedimento del Garante Privacy del 27/11/08.*

Modalità di implementazione: *Nomina degli incaricati al trattamento dei dati personali, individuazione e nomina ad amministratori di sistema e comunicazione delle nomine.*

Piano di implementazione: *Attuato*

Analisi e gestione del rischio in ambito infrastrutturale

Vantaggi dell'applicazione della metodologia

- Giustificazione degli investimenti nelle contromisure

- Approccio compatibile con i punti 6.1.2 (risk assessment) e 6.1.3 (risk treatment) della ISO27001:2013

- La prima parte del documento di gestione del rischio è auditabile e utilizzabile per monitorare l'avanzamento delle attività

Agenda

- Presentazione relatore
- Considerazioni iniziali
- Analisi e gestione del rischio in ambito infrastrutturale
- Analisi e gestione del rischio in ambito applicativo
- Q&A

Analisi e gestione del rischio in ambito applicativo

Una applicazione informatica è come una pistola

Può essere:

- scarica
- caricata a salve
- caricata con proiettili veri

Analisi e gestione del rischio in ambito applicativo

Nel caso di una applicazione informatica il rischio deve essere valutato in base ai dati gestiti

Devono essere valutate:

- riservatezza
- integrità
- disponibilità

Analisi e gestione del rischio in ambito applicativo

La ISO27001-2013 dice che:

A.14.2.1	Secure development policy	*Control* Rules for the development of software and systems shall be established and applied to developments within the organization.

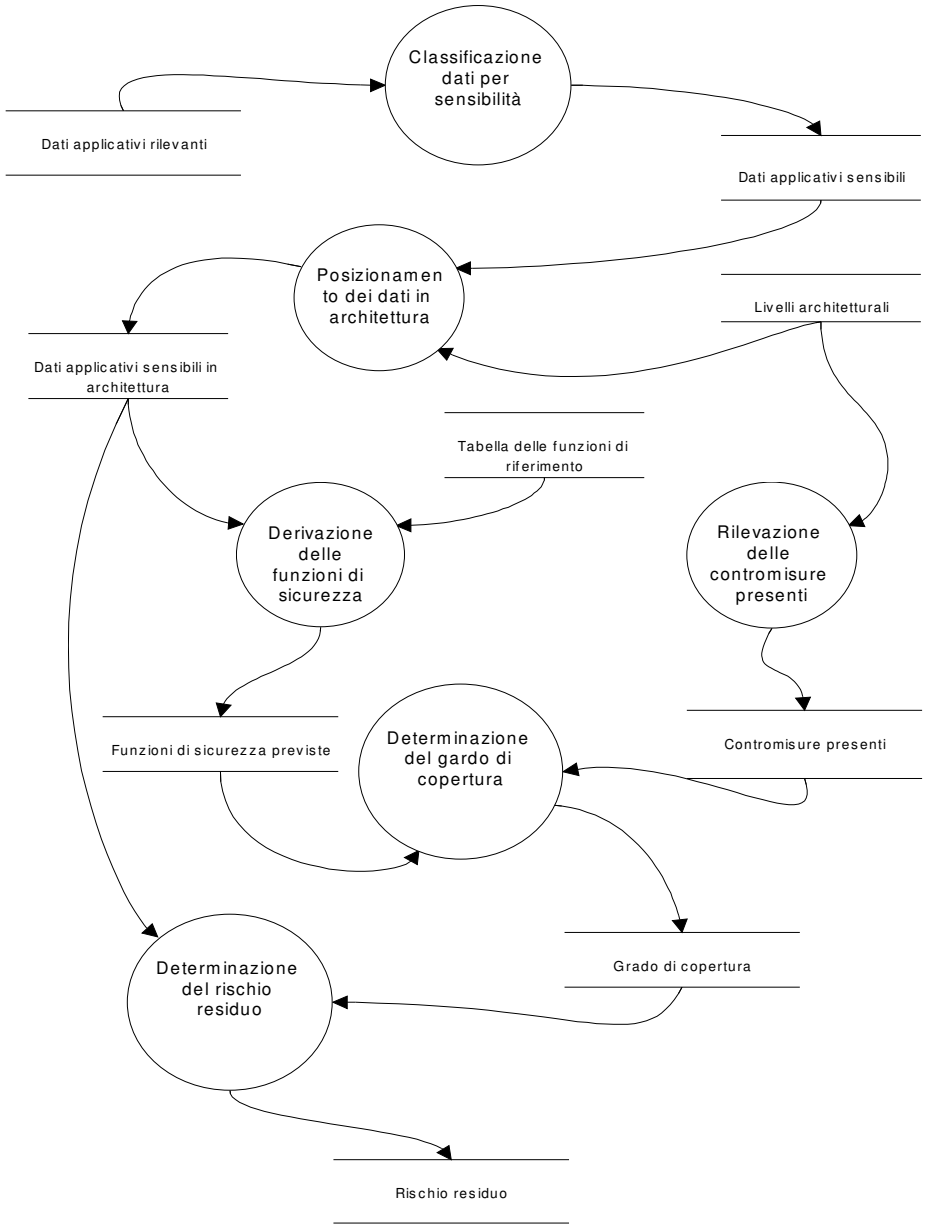
A.14.2.5	Secure system engineering principles	*Control* Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.

Analisi e gestione del rischio in ambito applicativo

Attività per la valutazione del rischio

- *Classificazione dati applicativi per sensibilità*
- *Posizionamento dati applicativi con relative classi di sensibilità in architettura*
- *Derivazione delle funzioni di sicurezza*
- *Rilevazione delle contromisure presenti*
- *Determinazione del grado di copertura*
- *Determinazione del rischio residuo*

Analisi e gestione del rischio in ambito applicativo



Analisi e gestione del rischio in ambito applicativo

Area di rischio

Si intende l'insieme delle seguenti informazioni: classe di sensibilità del dato, parametro di sicurezza, livello architetturale

Classe di sensibilità

*Accoglie i dati con esigenze di protezione analoghe riguardo alla loro **I**ntegrità, **R**iservatezza e **D**isponibilità.*
Sono previste tre classi di sensibilità:

- ***A**lta;*
- ***M**edia;*
- ***B**assa.*

Analisi e gestione del rischio in ambito applicativo

Grado di copertura

Indica, per un livello architetturale e per una determinata classe di sensibilità dei dati, la percentuale delle funzioni di sicurezza presenti ed utilizzate rispetto a quelle previste nella politica di sicurezza. Il grado di copertura è espresso secondo i seguenti valori:

- ***A**lto;*
- ***M**edio;*
- ***B**asso.*

Analisi e gestione del rischio in ambito applicativo

Parametri di sicurezza

Parametri per la classificazione della rilevanza dei dati.
*Tali parametri sono: **I**ntegrità, **R**iservatezza, **D**isponibilità.*

Analisi e gestione del rischio in ambito applicativo

Rischio residuo

Classifica le aree di rischio su cui si deve intervenire prioritariamente. Tale classificazione viene effettuata in base al grado di copertura e alla classe di sensibilità del dato. E' prevista una scala di quattro valori numerici (da 1 a 4).

Analisi e gestione del rischio in ambito applicativo

Criticità dei dati

La criticità di ogni dato (macroentità) è la combinazione di importanza e rilevanza: è la **sensibilità** del dato

Importanza è la valenza aziendale ovvero quanto il dato è importante per il business (valori: basso, medio, alto)

Rilevanza è la criticità del dato nei confronti di riservatezza, integrità e disponibilità del dato (valori: 1, 2, 3)

Analisi e gestione del rischio in ambito applicativo

Come rilevare l'importanza

Metodo induttivo

Metodo deduttivo

Analisi e gestione del rischio in ambito applicativo

Come rilevare l'importanza (metodo induttivo)

1) Valutare la criticità dei processi rispetto alla contribuzione al successo aziendale

Determinant	5	10	15	20	25
Relevant	4	8	12	16	20
Influent	3	6	9	12	15
Little influent	2	4	6	8	10
Marginal	1	2	3	4	5
	General structure	**Control structure**	**support to management**	**Support to mission**	**Company mission**

Analisi e gestione del rischio in ambito applicativo

Come rilevare l'importanza (metodo induttivo)

2) Correlare la criticità dei processi ai dati per ricavare l'importanza dei dati

Macro-entità / Processi	valore del processo	anagrafe cliente	tassazione	domanda /prodotto e servizio per cliente	modulo tariffario	anagrafica centrale
Customer care	20	**X**	**X**	**X**		
Business Sales & management	20	**X**		**X**	**X**	
Fatturazione e gestione crediti	15	**X**	**X**	**X**	**X**	
Esercizio	25		**X**			**X**
Gestione operativa traffico	20		**X**			**X**
Controllo compatibilità legislativa	15	**X**	**X**	**X**		
TOTALI DI IMPORTANZA		**70**	**95**	**70**	**35**	**45**

Analisi e gestione del rischio in ambito applicativo

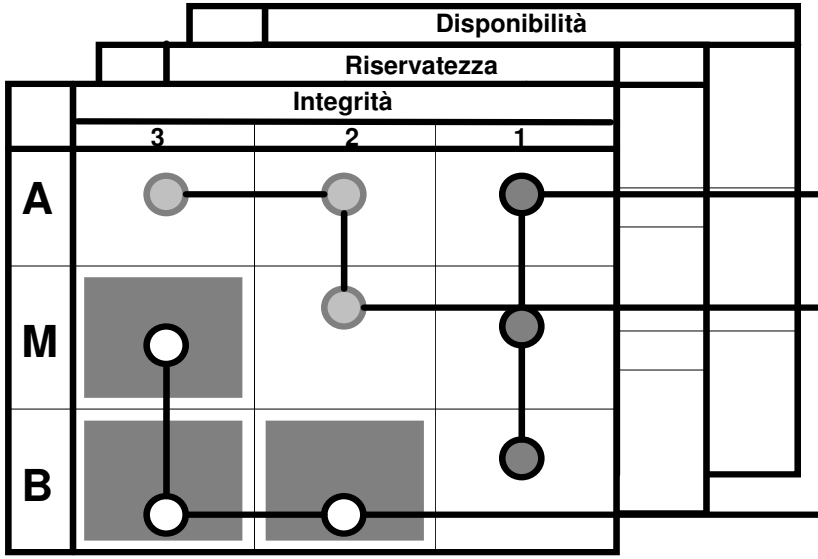
Come rilevare l'importanza (metodo deduttivo)

Correlare l'importanza dei dati al danno

Classe	Descrizione delle conseguenze
A	Perdita di immagine (Istituzionale/internazionale/nazionale) Perdita di business Implicazioni penali Esclusione dai mercati mobiliari Mancate certificazioni (bilancio, qualità, antimafia, ecc.) Perdite finanziarie irreversibili e consistenti Violazione segreti di missione/leggi Violazione norme antitrust Violazione norme comunitarie Alterazione sistemi di controllo
M	Apertura contenziosi sul mercato (clienti/fornitori) Perdite sul mercato mobiliare Sanzioni amministrative Perdite finanziari assorbibili Contenzioso con i dipendenti Alterazione consistenza patrimoniale (per efficacia) Alterazione dei sistemi di controllo di gestione
B	Perdite temporanee di efficienza Alterazione dei sistemi di gestione ordinaria Perdite finanziarie recuperabili Violazione norme aziendali di gestione Alterazione consistenza patrimoniale (per efficienza)

Analisi e gestione del rischio in ambito applicativo

Sensibilità dei dati



Condizioni possibili

Il valore esprime delle condizioni di bassa rilevanza e quindi non determinanti ai fini della sicurezza perchè risolte nel contesto di gestione

Condizioni pertinenti

Il valore esprime delle condizioni di sensibilità medio/alta, quindi individua l'area su cui maggiormente agisce il sistema della sicurezza

Condizioni aderenti

Il valore esprime delle condizioni di sensibilità medio/bassaa, quindi individua l'area su cui il sistema della sicurezza agisce marginalmente

Analisi e gestione del rischio in ambito applicativo

Valori della sensibilità dei dati

		RILEVANZA								
		Integrità			Riservatezza			Disponibilità		
		3	2	1	3	2	1	3	2	1
IMPORTANZA	A	Alta	Alta	Media	Alta	Alta	Media	Alta	Alta	Media
	M	Media	Media	Bassa	Media	Media	Bassa	Media	Media	Bassa
	B	Bassa	Bassa	Bassa	Bassa	Bassa	Bassa	Bassa	Bassa	Bassa

Sensibilità	*Importanza - Rilevanza*			
Alta	A-3	A-2		
Media	A-1	M-3	M-2	
Bassa	M-1	B-3	B-2	B-1

Analisi e gestione del rischio in ambito applicativo

Modulo per la classificazione della sensibilità dei dati

xxxxxx	codice progetto	descrizione progetto
data di rilevazione	nome analisti	
--/--/----		

Dati	Importanza	Rilevanza per Integrità	Rilevanza per Riservatezza	Rilevanza per Disponibilità	Sensibilità per Integrità	Sensibilità per Riservatezza	Sensibilità per Disponibilità

Note

Funzioni di sicurezza

CLASSI DI FUNZIONI DI SICUREZZA SOFTWARE/HARDWARE

Identificazione/Autenticazione: *stabilisce e verifica l'identità dichiarata da un utente che vuole accedere al sistema. Il sistema deve identificare e autenticare univocamente gli utenti che intendono accedere al sistema. L'identificazione e l'autenticazione devono essere effettuate prima di ulteriori interazioni tra la rete e l'utente. Si potranno avere altre interazioni con la rete solo dopo che l'operazione di identificazione e autenticazione è andata a buon fine. Le informazioni di autenticazione devono essere memorizzate in maniera che possano essere accedute solo da utenti autorizzati*

Funzioni di sicurezza

CLASSI DI FUNZIONI DI SICUREZZA SOFTWARE/HARDWARE

Controllo autorizzazione alle funzionalità/servizi: *garantisce che un utente possa espletare le sole operazioni di sua competenza. Tra tali funzionalità vanno previste quelle di amministrazione dei diritti di accesso e della loro verifica*

Controllo autorizzazione ai dati: *garantisce che il processo e/o utente possano operare solo sui dati di propria competenza. Tra tali funzioni vanno previste quelle di amministrazione dei diritti di accesso e della loro verifica*

Funzioni di sicurezza

CLASSI DI FUNZIONI DI SICUREZZA SOFTWARE/HARDWARE

***Tracciamento**: registra gli accessi alle varie risorse del sistema informatico rilevanti per gli aspetti di sicurezza. Non deve essere permesso agli utenti non autorizzati di accedere alle informazioni registrate. Deve essere inoltre possibile registrare selettivamente le azioni di uno o più utenti*

Funzioni di sicurezza

CLASSI DI FUNZIONI DI SICUREZZA SOFTWARE/HARDWARE

***Sistemi che evidenziano eventi anomali**: permettono di investigare sugli eventi che, discostandosi da determinate soglie, possono rappresentare una minaccia alla sicurezza. Devono essere presenti e documentati appositi strumenti per esaminare e gestire gli archivi registrati. Tali strumenti devono consentire di identificare selettivamente le azioni eseguite da uno o più utenti. Periodicamente controllano le registrazioni, per verificare casi anomali o sospetti. Permettono l'Alert on-line o differito al superamento di opportune soglie di sicurezza predefinite*

Funzioni di sicurezza

CLASSI DI FUNZIONI DI SICUREZZA SOFTWARE/HARDWARE

Oscuramento dati d'archivio*: offre la possibilità di cifrare i dati al fine di garantirne la riservatezza*

Sistemi di riutilizzo supporti magnetici*: gestiscono il riutilizzo di risorse. Fra queste funzioni vi sono quelle di inizializzazione e cancellazione di supporti asportabili e riusabili, quali nastri magnetici e dischetti, o di gestione di supporti in output, come la cancellazione della schermata*

Analisi e gestione del rischio in ambito applicativo

Funzioni di sicurezza

CLASSI DI FUNZIONI DI SICUREZZA SOFTWARE/HARDWARE

Rilevazione e ripristino affidabilità software*: permettono l'analisi del software al fine di identificare, segnalare e correggere violazioni all'integrità. Fra tali funzioni vi sono quelle di identificazione ed eliminazione dei virus, bombe logiche e "cavalli di troia", analisi del codice per verificare la correttezza delle chiamate ai dati, ecc*

Qualità dei dati*: costituisce un insieme di misure da intraprendere al fine di elevare la qualità dei dati, con particolare riferimento ai dati entranti nel sistema informatico aziendale. Tali misure consistono in funzioni di valorizzazione, funzioni di integrità semantica, funzioni di integrità referenziale, funzioni di integrità logica, funzioni di non ridondanza e funzioni di aggiornamento*

Analisi e gestione del rischio in ambito applicativo

Funzioni di sicurezza

CLASSI DI FUNZIONI DI SICUREZZA SOFTWARE/HARDWARE

Duplicazione dati/risorse*: garantisce la ridondanza dei dati e delle risorse al fine di un loro ripristino in caso di indisponibilità. Tra tali funzioni vi sono quelle di salvataggio periodico (backup), mirroring dei dischi, logging*

Controllo interscambio dati*: assicura la sicurezza nelle trasmissioni di dati attraverso: autenticazione dell'originatore, integrità e riservatezza del contenuto del messaggio, non ripudio dell'originatore e del destinatario*

Funzioni di sicurezza

CLASSI DI FUNZIONI DI SICUREZZA ORGANIZZATIVE

***Ruoli e responsabilità**: descrizione di figure aziendali operative che gestiscono aspetti di sicurezza evidenziando le responsabilità ed attività di loro competenza in ambito EDP*

***Norme di utilizzo**: documento rivolto agli utenti che descrive le norme comportamentali e procedurali da applicare per un utilizzo sicuro del sistema*

***Procedure di gestione**: documento rivolto agli addetti alla gestione degli aspetti di sicurezza del sistema che descrive le modalità di svolgimento delle attività di loro competenza*

Funzioni di sicurezza

CLASSI DI FUNZIONI DI SICUREZZA ORGANIZZATIVE

Formazione*: attività tesa a istruire gli addetti e gli utenti che operano su risorse sensibili al fine di utilizzare al meglio i dispositivi di sicurezza progettati e di far conoscere ed applicare la norma relativa*

Sensibilizzazione e comunicazione*: attività svolta verso tutti gli utenti per sensibilizzarli alle problematiche generali di sicurezza e alle relative norme*

Analisi e gestione del rischio in ambito applicativo

Funzioni di sicurezza

CLASSI DI FUNZIONI DI SICUREZZA LOGISTICHE

Sistemi di rilevazione passiva*: impianti che rilevano la presenza di situazioni logistiche anomale (incendio, allagamento, fumo), inviando uno specifico allarme ai centri di controllo senza attivare contromisure*

Sistemi di rilevazione attiva*: impianti che rilevano la presenza di situazioni logistiche anomale (incendio, allagamento, fumo), inviando uno specifico allarme ai centri di controllo e attivando una specifica contromisura*

Sistemi di controllo accessi fisici*: impianti che regolano l'accesso fisico in determinate aree riservate alle sole persone e mezzi autorizzati*

Funzioni di sicurezza

CLASSI DI FUNZIONI DI SICUREZZA LOGISTICHE

Sistemi di continuità di alimentazione*: impianti che garantiscono una continuità dell'alimentazione elettrica ai sistemi, almeno per una chiusura ordinata*

Infrastrutture*: accorgimenti generici sugli edifici e disposizione dei locali al fine di garantire la sicurezza (edifici antisismici, uscite di sicurezza allarmate, separazione ambienti a rischio, ecc.)*

Analisi e gestione del rischio in ambito applicativo

Relazioni tra sensibilità e funzioni di sicurezza

	Classe di sensibilità / Parametro di Sicurezza / Funzioni di Sicurezza	ALTA			MEDIA			BASSA		
		I	R	D	I	R	D	I	R	D
HW/SW	Controllo accesso/collegamento logico	X	X		X	X		X	X	
	Controllo autorizzazione alle funzioni/servizi	X	X		X	X		X	X	
	Controllo autorizzazione ai dati	X	X		X	X		X	X	
	Tracciamento	X	X	X	X	X	X			
	Sistemi che evidenziano eventi anomali	X	X	X	X	X	X			
	Crittografia		X							
	Sistemi riutilizzo supporti magnetici (object reuse)		X							
	Rilevazione e ripristino affidabilita' sw e dati	X			X			X		
	Duplicazione dei dati/risorse			X			X			X
	Controllo interscambio dati	X	X		X	X				
ORG	Norme di utilizzo	X	X	X	X	X	X			
	Procedure di gestione	X	X	X	X	X	X			
	Ruoli e responsabilità	X	X	X	X	X	X	X	X	X
	Formazione	X	X	X						
	Sensibilizzazione e comunicazione	X	X	X	X	X	X	X	X	X
LOG	Sistemi di rilevazione passiva			X			X			
	Sistemi di rilevazione attiva			X			X			
	Sistemi di controllo accessi fisici	X	X	X	X	X	X			
	Sistemi di continuità di alimentazione	X		X	X		X			
	Infrastrutture			X			X			

Analisi e gestione del rischio in ambito applicativo

Livelli di copertura

Per ogni livello di sensibilità nei confronti di ogni elemento della terna RID andranno determinate le funzioni di sicurezza presenti e quelle assenti

Il livello di copertura sarà definito dalla percentuale di funzioni di sicurezza presenti rispetto a quelle possibili

0 - 30 %	**BASSO**
31 - 60 %	**MEDIO**
61 - 100 %	**ALTO**

Analisi e gestione del rischio in ambito applicativo

Livelli di copertura

Le caselle di correlazione tra le funzioni di sicurezza e le classi di sensibilità dei dati applicativi devono essere contrassegnate col simbolo "○" se si vuole indicare l'assenza della relativa funzione, oppure col simbolo "●" qualora se ne voglia indicare la presenza

Analisi e gestione del rischio in ambito applicativo

Livelli di copertura - Esempio

Classe di sensibilità	ALTA			MEDIA			BASSA		
Parametro di Sicurezza / Funzioni di Sicurezza	I	R	D	I	R	D	I	R	D
Identificazione/Autenticazione	○	○		○	○		○	○	
Controllo autorizzazione alle funzioni/servizi	●	●		●	●		●	●	
Controllo autorizzazione ai dati	○	○		○	○		○	○	
Tracciamento	●	●	●	●	●	●			
Sistemi che evidenziano eventi anomali	●	●	●	●	●	●			
Oscuramento dati d'archivio		○							
Sistemi riutilizzo supporti magnetici		○							
Rilevazione e ripristino affidabilità sw	●			●			●		
Qualità dei dati	○			○			○		
Duplicazione dei dati/risorse			●			●			●
Controllo interscambio dati	○	○		○	○				
Norme di utilizzo	○	○	○	●	●	●			
Procedure di gestione	○	○	○	●	●	●			
Ruoli e responsabilità	○	○	○	●	●	●	●	●	●
Formazione	●	●	●						
Sensibilizzazione e comunicazione	○	○	○	●	●	●	●	●	●
Sistemi di rilevazione passiva			●			●			
Sistemi di rilevazione attiva			○			○			
Sistemi di controllo accessi fisici	○	○	○	○	○	○			
Sistemi di continuità di alimentazione	●		●	●		●			
Infrastrutture			●			●			
	6/15	4/14	7/13	9/14	7/11	10/12	4/7	3/5	3/3
GRADO DI COPERTURA	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	Alto

Analisi e gestione del rischio in ambito applicativo

Determinazione del rischio residuo

Fissando una serie di valori discreti del rischio crescenti da 1 a 4, si potrà correlare il rischio residuo al grado di copertura

Classe di sensibilità / Grado di copertura	ALTA	MEDIA	BASSA
ALTO	**Rischio = 1**	**Rischio = 1**	**Rischio = 1**
MEDIO	**Rischio = 3**	**Rischio = 2**	**Rischio = 1**
BASSO	**Rischio = 4**	**Rischio = 3**	**Rischio = 1**

Analisi e gestione del rischio in ambito applicativo

Livelli architetturali

Spesso le applicazioni insistono su più livelli architetturali così come i dati gestiti

- Host
- Rete
- Sistemi dipartimentali
- Workstation
- Supporti di backup

Analisi e gestione del rischio in ambito applicativo

Livelli architetturali

E’ necessario gestire i livelli architetturali presenti in azienda e per ogni livello i meccanismi applicabili a quel livello per ogni funzione di sicurezza

Analisi e gestione del rischio in ambito applicativo

Livelli architetturali

	Funzioni di Sicurezza	xxx	Yyy
HW/SW	Identificazione/Autenticazione		
	Controllo autorizzazione alle funzioni/servizi		
	Controllo autorizzazione ai dati		
	Tracciamento		
	Sistemi che evidenziano eventi anomali		
	Oscuramento dati d'archivio		
	Sistemi riutilizzo supporti magnetici (object reuse)		
	Rilevazione e ripristino affidabilità' sw e dati		
	Duplicazione dei dati/risorse		
	Controllo interscambio dati		
ORG	Norme di utilizzo		
	Procedure di gestione		
	Ruoli e responsabilità		
	Formazione		
	Sensibilizzazione e comunicazione		
LOG	Sistemi di rilevazione passiva		
	Sistemi di rilevazione attiva		
	Sistemi di controllo accessi fisici		
	Sistemi di continuità di alimentazione		
	Infrastrutture		

Analisi e gestione del rischio in ambito applicativo

Livelli architetturali

Il calcolo del rischio e del livello di copertura dovrà essere effettuato per tutti i livelli architetturali che riguardano l'applicazione

Analisi e gestione del rischio in ambito applicativo

Applicazioni esistenti e applicazioni da sviluppare

I passi da compiere per analizzare una applicazione esistente oppure per applicare l'analisi in fase di progettazione sono concettualmente diversi

Analisi e gestione del rischio in ambito applicativo

Per una applicazione esistente

- *Rilevazione, in termini di prodotti/meccanismi, delle **contromisure** presenti sui pertinenti livelli architetturali del sistema informatico ove l'applicazione viene gestita*

- *Rilevazione delle funzioni di sicurezza che ciascun meccanismo/prodotto offre, verificando in particolare l'esistenza delle apposite strutture organizzative*

Analisi e gestione del rischio in ambito applicativo

Per una applicazione esistente

- *Rilevazione di quali siano i servizi, tra quelli presenti nel meccanismo/prodotto, che risultano effettivamente implementati*

- *Determinazione del grado di copertura delle contromisure attuali nell'ambito dei vari livelli architetturali determinando il valore di* ***rischio residuo*** *tramite la differenza per "difetto" fra le funzioni implementate e quelle di riferimento per ciascuna classe di sensibilità.*

Analisi e gestione del rischio in ambito applicativo

Per una applicazione da sviluppare

- *Determinazione della sensibilità dei dati da gestire, e loro posizionamento nei livelli architetturali coinvolti*

- *Rilevazione di quali funzioni di sicurezza offrono i meccanismi/prodotti presenti sui livelli architetturali coinvolti (dove si progetta la nuova applicazione), verificando l'esistenza delle strutture organizzative previste*

Analisi e gestione del rischio in ambito applicativo

Per una applicazione da sviluppare

- *Valutazione della robustezza di ciascun meccanismo/prodotto per ogni funzione che esso offre. Se ci sono delle discrepanze per difetto con la politica di sicurezza e si decide di acquisire/sviluppare una nuova tecnologia per soddisfare i requisiti, anch'essa deve essere valutata in termini di robustezza*

- *Utilizzo delle funzioni esistenti e eventuale implementazione di quelle mancanti acquistando/sviluppando i relativi prodotti ed introducendo le apposite strutture organizzative*

Analisi e gestione del rischio in ambito applicativo

Vantaggi dell'applicazione della metodologia

- Giustificazione degli investimenti nelle contromisure
- Approccio compatibile con i punti A.14.2.1 e A.14.2.5 della ISO27001:2013
- Applicabile per nuovi progetti e per progetti in esercizio

Agenda

- Presentazione relatore
- Considerazioni iniziali
- Analisi e gestione del rischio in ambito infrastrutturale
- Analisi e gestione del rischio in ambito applicativo
- Q&A

Q &A

Domande?

Contatti

m.mistre@isacaroma.it

Grazie...