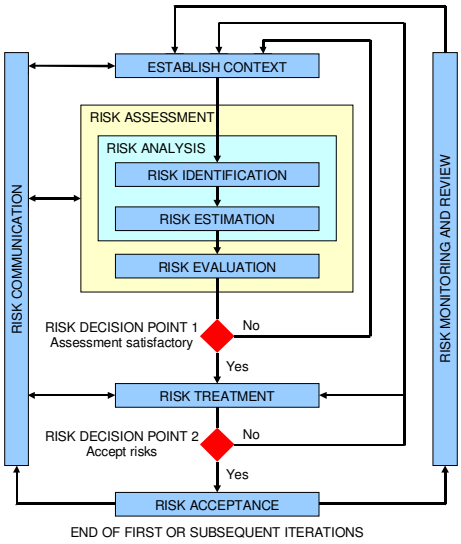
Il processo di analisi dei rischi (parte II)

Marco Domenico Aime
< m.aime @ polito.it >

Politecnico di Torino
Dip. di Automatica e Informatica

1

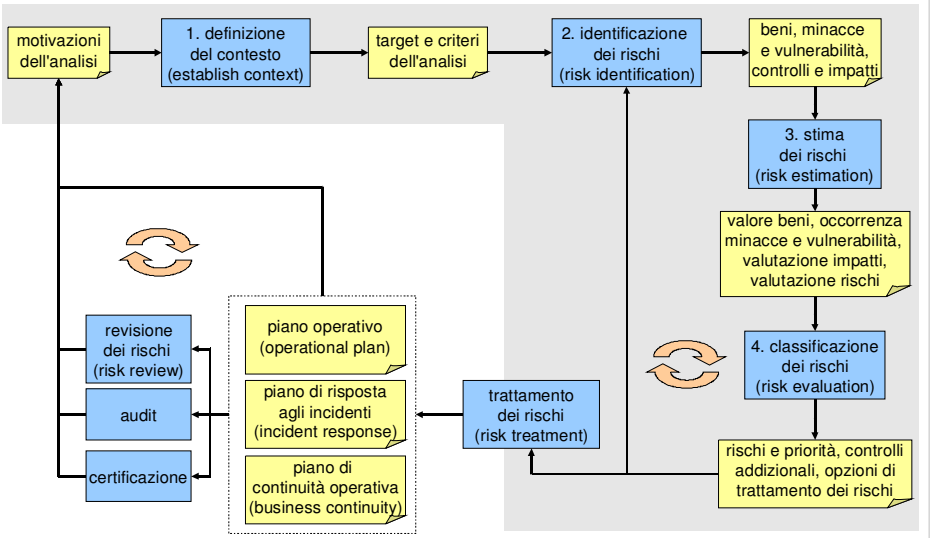
Il processo di gestione dei rischi



fonte: ISO 27005

2

Il processo di gestione dei rischi



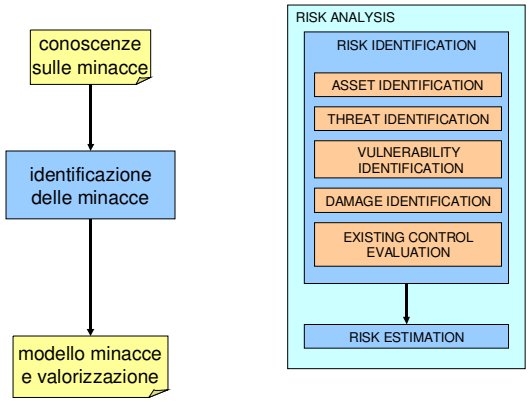
3

2.1.2. Identificazione delle minacce (Threat identification)

- **minaccia:**
  - la causa potenziale di un incidente che può provocare danno a uno o più beni (cfr. ISO 27001)
  - eventi che possono causare un incidente nell'organizzazione, producendo danni materiali e perdite immateriali nei suoi beni (cfr. MAGERIT v2)
  - la potezialità che una sorgente di minaccia eserciti (attivi accidentalmente o sfrutti intenzionalmente) una specifica vulnerabiltà (cfr. SP 800-30)
- **durante il funzionamento (runtime) del sistema una minaccia si può concretizzare in un incidente**
  - sfruttando una o più vulnerabilità

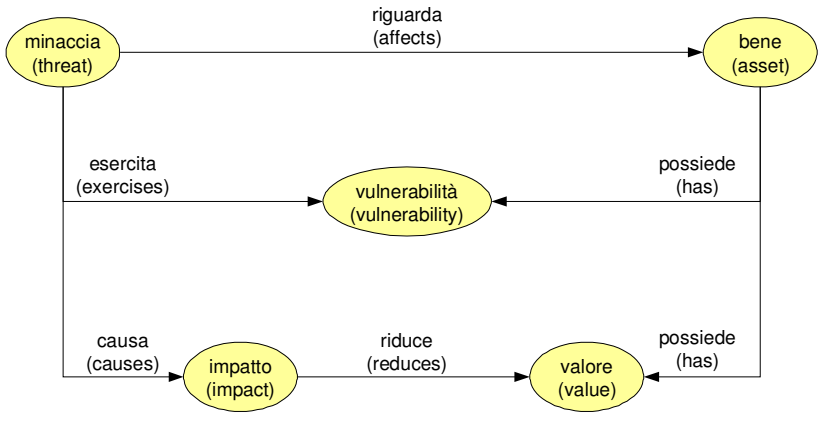
5

2.1.2. Identificazione delle minacce



6

Modello dei rischi (beni - minacce - vulnerabilità)



7

Minacce e vulnerabilità

- **perché differenziare minacce e vulnerabilità?**
  - distinguere tra possibilità e facilità di riuscita
    - es. rubare un'auto con antifurto satellitare
  - distinguere tra possibilità e frequenza/probabilità
    - es. intercettare una telefonata
  - distinguere tra fine e mezzi
    - es. aprire una porta con l'esplosivo

8

Associazione minacce e vulnerabilità

- **la presenza di una vulnerabilità non può causare danno di per se: deve essere presente una minaccia che la sfrutta**
  - es. un dato non crittografato ma non interessante
- **lo scopo dei controlli è diminure la vulnerabilità dei beni alle varie minacce**
  - un controllo non correttamente implementato o malfunzionante può esso stesso costituire una vulnerabiltà (ricorsione)

9

Associazione minacce e vulnerabilità

- **una minaccia senza vulnerabilità non richiede l'implementazione di controlli addizionali**
  - problema del livello di protezione
    - efficacia dei controlli < 100%
  - problema delle vulnerabilità non note
  - problema delle nuove vulnerabilità
  - in ogni caso dobbiamo identificarla e tenerla sotto osservazione

10

Associazione minacce e vulnerabilità

- **una vulnerabilità senza minacce corrispondenti può non richiedere controlli addizionali**
  - problema dell'opportunità
    - facilità nel rieseguire attacchi noti, un attacco può provenire da tutte le parti del pianeta
  - problema del valore
    - un bene di poco valore per me può avere valore per altri (es. botnet)
  - in ogni caso dobbiamo identificarla e tenerla sotto osservazione

11

Associazione minacce e vulnerabilità

- **una minaccia può esercitare più vulnerabilità**
- **una vulnerabilità può essere esercitata da più minacce**

Vulnerability	Threat-Source	Threat Action
Data center uses water sprinklers to suppress fire; tarpaulins to protect hardware and equipment from water damage are not in place	Fire, negligent persons	Water sprinklers being turned on in the data center

fonte: NIST SP 800-30, pp 15-16

12

Minacce e vulnerabilità

- **nella pratica, alcune metodologie non distinguono**
- **in alcune prevale il concetto di minaccia:**
  - il concetto di vulnerabilità è modellato implicitamente nella valorizzazione della minaccia
- **in altre prevale il concetto di vulnerabilità:**
  - le minacce sono modellate come categorie o come aggeragazioni (unione, sequenza) di vulnerabilità

13

Conoscenza delle minacce

- **fonti interne all'organizzazione:**
  - proprietari o utenti di uno specifico bene
  - esperti dei sistemi informativi e della sicurezza
  - amministratori dei sistemi informativi
  - processi di monitoraggio e gestione incidenti
- **fonti esterne:**
  - autorità governative o private possono fornire cataloghi e statistiche sulle minacce
    - generali o per tipo di organizzazione / business
  - società assicurative

14

Conoscenza delle minacce

- **le minacce sono in continua evoluzione:**
  - fare attenzione quando si usano cataloghi e/o risultati di precedenti analisi
  - in genere le fonti interne hanno rilevanza maggiore
  - i cataloghi sono da intendere come suggerimenti su cosa bisogna considerare per tipologia di bene e dimensione di sicurezza
- **l'esperienza dell'analista è ancora un fattore fondamentale**

15

Esempi di fonti esterne

- **organismi di Computer Emergency Response**
  - es. CERT.org, US-CERT.gov, GovCERT.it
- **organismi di standardizzazione**
  - es. NIST.gov, MITRE.org
- **organizzazioni di sensibilizzazione**
  - es. OWASP.org, SANS.org
- **mass media e specialmente risorse web**
  - es. SecurityFocus.com, SecurityWatch.com, SecurityPortal.com

16

Modello delle minacce

- **una minaccia è caratterizzata da**
  - categoria/tipo e descrizione
  - tipi di beni interessati
  - dimensioni di sicurezza interessate
  - sorgente/attore
  - modalità/azioni/accesso
- **la maggior parte delle metodologie usa delle liste predefinite**
- **le tecniche più moderne forniscono criteri per identificare le minacce a partire dal modello strutturato del sistema**

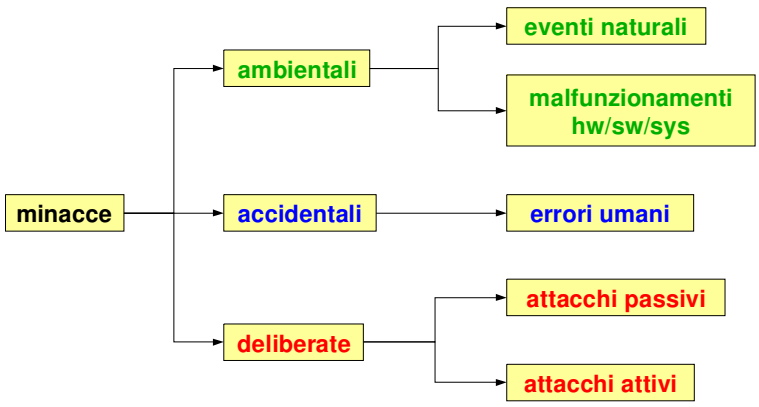
18

Tipi di minacce

- **una minaccia può essere**
  - di origine naturale o umana
  - deliberata o accidentale
- **le minacce deliberate sono particolarmente difficili da modellare**
  - tendono a sfuggire ad una trattazione statistica
  - “la sicurezza complessiva è pari a quella dell'anello più debole”

19

Tipi di minacce



20

Relazione tra errori e attacchi

- **alcuni errori e attacchi hanno in comune effetti e modalità**
  - lo stesso danno può interessare un bene accidentalmente oppure deliberatamente

fonte: MAGERIT v2, catalogo, pp 40-41 (english version)

number	error	attack
1	Users' errors	
2	Administrator errors	
3	Monitoring (logging) errors	
4	Configuration errors	Manipulation of the configuration
5		Masquerading of user identity
6		Abuse of access privileges
7	Organisational deficiencies	Misuse
8	Malware diffusion	Malware diffusion
9	[Re-]routing errors	[Re-]routing of messages
10	Sequence errors	Sequence alteration
11		Unauthorised access
12		Traffic analysis
13		Repudiation
14	Information leaks	Eavesdropping
15	Information alteration	Alteration of information
16	Entry of incorrect information	Entry of false information
17	Information degradation	Corruption of information
18	Destruction of information	Destruction of information
19	Disclosure of information	Disclosure of information
20	Software vulnerabilities	
21	Defects in software maintenance / updating	
22		Software manipulation
23	Defects in hardware maintenance / updating	
24	System failure due to exhaustion of resources	Denial of service
25		Theft
26		Destructive attack
27		Enemy over-run
28	Staff shortage	Staff shortage
29		Extortion
30		Social engineering

21

Fonti di minacce deliberate

- **utili per distinguere la concretezza di una minaccia in base al tipo e quantità di mezzi richiesti**

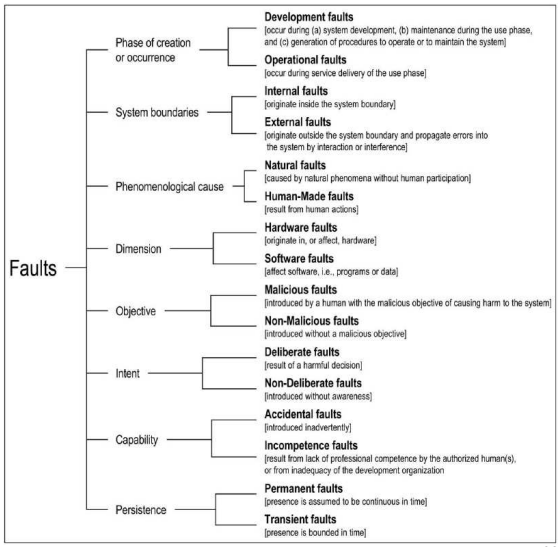
fonte: NIST SP 800-30, pp. 14

Threat-Source	Motivation	Threat Actions
Hacker, cracker	Challenge Ego Rebellion	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay, impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	• Bomb/Terrorism • Information warfare • System attack (e.g., distributed denial of service) • System penetration • System tampering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access(access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g., virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

Tassonomia dei fault

- **tassonomia di alto livello**
- **ottimo riferimento, ma non aiuta nell'identificazione e valorizzazione pratica delle minacce**

fonte: Avizienis, Laprie, Randell, Landwher, "Basic Concepts and Taxonomy of Dependable and Secure Computing", IEEE TDSC, 2004



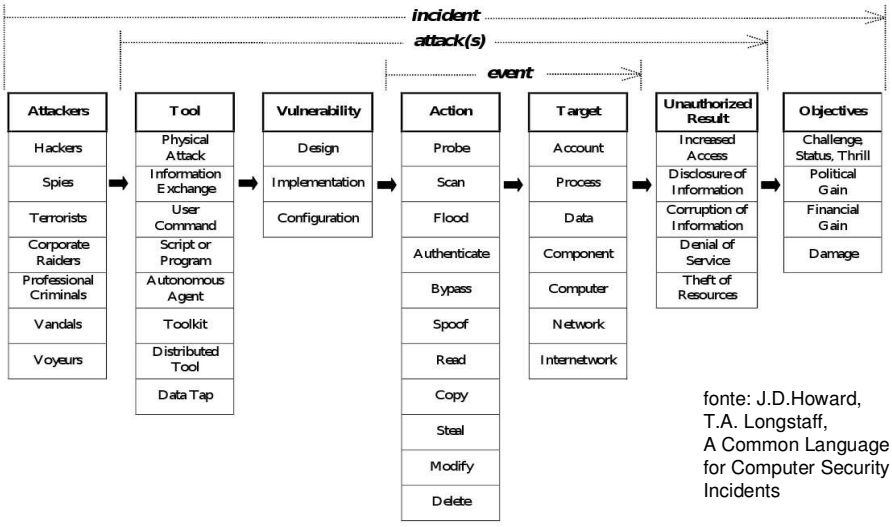
23

Tassonomia incidenti

- **svariate**
- **una delle più note:**
  - Howard, J.D. and Longstaff, T.A., A Common Language for Computer Security Incidents, (SAND98-8667), Sandia National Laboratories, 1998 http://www.cert.org/research/taxonomy_988667.pdf
- **ottimi riferimenti, ma non aiutano direttamente nell'identificazione e valorizzazione pratica delle minacce**

25

Tassonomia incidenti per computer e reti



fonte: J.D.Howard, T.A. Longstaff, A Common Language for Computer Security Incidents

26

Cataloghi di minacce: ISO 27005

- **basati su categorie**
- **usati dalle metodologie classiche**

Type	Threats	Origin
	Software malfunction	A
	Breach of information system maintainability	A, D
Unauthorised actions	Unauthorised use of equipment	D
	Fraudulent copying of software	D
	Use of counterfeit or copied software	A, D
	Corruption of data	D
	Illegal processing of data	D
Compromise of functions	Error in use	A
	Abuse of rights	A, D
	Forging of rights	D
	Denial of actions	D
	Breach of personnel availability	A, D, E

D (deliberate) = deliberate
A (accidental) = umane ma accidentali
E (environmental) = non prevedono azioni umane

fonte: ISO 27005

Type	Threats	Origin
Physical damage	Fire	A, D, E
	Water damage	A, D, E
	Pollution	A, D, E
	Major accident	A, D, E
	Destruction of equipment or media	A, D, E
Natural events	Climatic phenomenon	E
	Seismic phenomenon	E
	Volcanic phenomenon	E
	Meteorological phenomenon	D, E
	Flood	E
Loss of essential services	Failure of air-conditioning	A, D
	Loss of power supply	A, D, E
	Failure of telecommunication equipment	A, D
Disturbance due to radiation	Electromagnetic radiation	A, D, E
	Thermal radiation	A, D, E
	Electromagnetic pulses	A, D, E
Compromise of information	Interception of compromising interference signals	D
	Remote spying	D
	Eavesdropping	D
	Theft of media or documents	A, D
	Theft of equipment	A, D
	Retrieval of recycled or discarded media	D
	Disclosure	A, D
	Data from untrustworthy sources	A, D
	Tampering with hardware	D
	Tampering with software	A, D
	Position detection	D
Technical failures	Equipment failure	A
	Equipment malfunction	A
	Saturation of the information system	A, D

27

Cataloghi di minacce: MAGERIT

- **[N] natural disaster**
  - Events that may occur without being directly or indirectly caused by human beings
- **[I] Of industrial origin**
  - Events that may occur accidentally arising from human activity of an industrial type. These threats may be accidental or deliberate
- **[E] Errors and unintentional failures**
  - Unintentional failures caused by persons
- **[A] Wilful attacks**
  - Deliberate failures caused by persons

fonte: MAGERIT v2, catalogo, pp. 26-40 (english version)

28

[N.1] Fire

Types of assets:	Dimensions:
[HW] computer equipment (hardware) [COM] communication networks [SI] media [AUX] auxiliary equipment [L] installations	1. [D] availability 2. [T_S] accountability of service use 3. [T_D] accountability of data access

Description:
Fires: possibility that the fire destroys system resources.

[N.2] Water damage

Types of assets:	Dimensions:
[HW] computer equipment (hardware) [COM] communication networks [SI] media [AUX] auxiliary equipment [L] installations	1. [D] availability 2. [T_S] accountability of service use 3. [T_D] accountability of data access

Description:
Floods: possibility that the water destroys system resources.

[N.*] Natural disasters

Types of assets:	Dimensions:
[HW] computer equipment (hardware) [COM] communication networks [SI] media [AUX] auxiliary equipment [L] installations	1. [D] availability 2. [T_S] accountability of service use 3. [T_D] accountability of data access

Description:
Other incidents that occur without human involvement: lightning, electric storm, earthquake, cyclones, avalanche, landslide, etc. ...
This excludes specific disasters such as fires (see [N.1]) and floods (see [N.2]).
This excludes personnel for whom there is a specific threat [E.31] to cover involuntary non-availability of personnel without going into its causes.

[I.1] Fire

Types of assets:	Dimensions:
[HW] computer equipment (hardware) [COM] communication networks [SI] media [AUX] auxiliary equipment [L] installations	1. [D] availability 2. [T_S] accountability of service use 3. [T_D] accountability of data access

Description:
Fire: possibility that the fire destroys the system's resources.

[I.2] Water damage

Types of assets:	Dimensions:
[HW] computer equipment (hardware) [COM] communication networks [SI] media [AUX] auxiliary equipment [L] installations	1. [D] availability 2. [T_S] accountability of service use 3. [T_D] accountability of data access

Description:
Escapes, leaks, floods: possibility that the water destroys the system's resources.

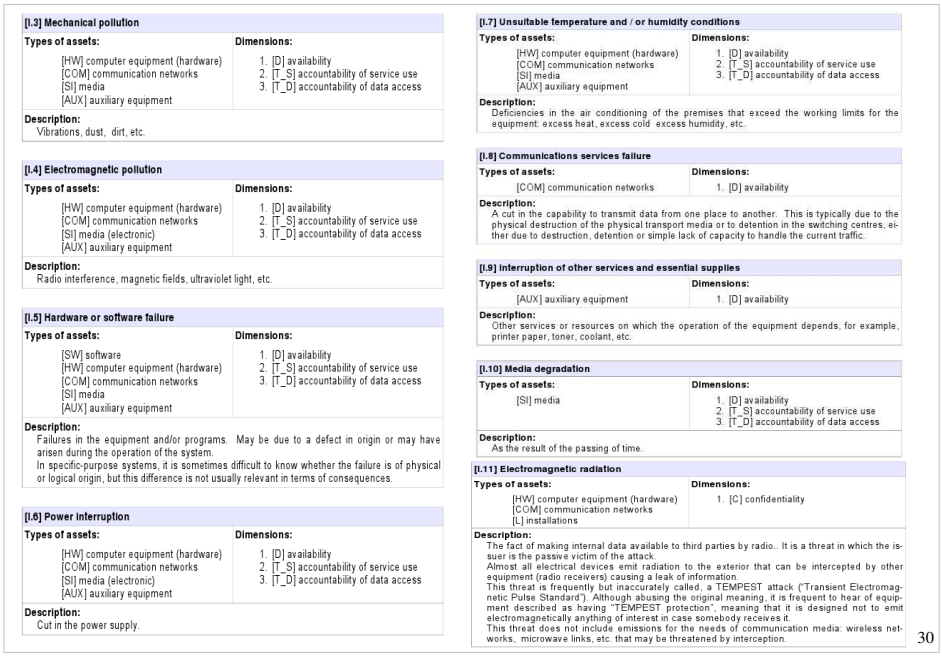
[I.*] Industrial disasters

Types of assets:	Dimensions:
[HW] computer equipment (hardware) [COM] communication networks [SI] media [AUX] auxiliary equipment [L] installations	1. [D] availability 2. [T_S] accountability of service use 3. [T_D] accountability of data access

Description:
Other disasters due to human activity: explosions, collapses, ...
- chemical pollution, ...
- electrical overloads, electrical fluctuations, ...
- traffic accidents, etc.

This excludes specific threats such as fire (see [I.1]) and flood (see [I.2]).
This excludes personnel for whom there is a specific threat [E.31], to cover involuntary non-availability of personnel without going into its causes.

29



[I.3] Mechanical pollution

Types of assets:	Dimensions:
[HW] computer equipment (hardware) [COM] communication networks [SI] media [AUX] auxiliary equipment	1. [D] availability 2. [T_S] accountability of service use 3. [T_D] accountability of data access

Description:
Vibrations, dust, dirt, etc.

[I.4] Electromagnetic pollution

Types of assets:	Dimensions:
[HW] computer equipment (hardware) [COM] communication networks [SI] media (electronic) [AUX] auxiliary equipment	1. [D] availability 2. [T_S] accountability of service use 3. [T_D] accountability of data access

Description:
Radio interference, magnetic fields, ultraviolet light, etc.

[I.5] Hardware or software failure

Types of assets:	Dimensions:
[SW] software [HW] computer equipment (hardware) [COM] communication networks [SI] media [AUX] auxiliary equipment	1. [D] availability 2. [T_S] accountability of service use 3. [T_D] accountability of data access

Description:
Failures in the equipment and/or programs. May be due to a defect in origin or may have arisen during the operation of the system.
In specific-purpose systems, it is sometimes difficult to know whether the failure is of physical or logical origin, but this difference is not usually relevant in terms of consequences.

[I.6] Power interruption

Types of assets:	Dimensions:
[HW] computer equipment (hardware) [COM] communication networks [SI] media (electronic) [AUX] auxiliary equipment	1. [D] availability 2. [T_S] accountability of service use 3. [T_D] accountability of data access

Description:
Cut in the power supply.

[I.7] Unsuitable temperature and / or humidity conditions

Types of assets:	Dimensions:
[HW] computer equipment (hardware) [COM] communication networks [SI] media [AUX] auxiliary equipment	1. [D] availability 2. [T_S] accountability of service use 3. [T_D] accountability of data access

Description:
Deficiencies in the air conditioning of the premises that exceed the working limits for the equipment: excess heat, excess cold excess humidity, etc.

[I.8] Communications services failure

Types of assets:	Dimensions:
[COM] communication networks	1. [D] availability

Description:
A cut in the capability to transmit data from one place to another. This is typically due to the physical destruction of the physical transport media or to detention in the switching centres, either due to destruction, detention or simple lack of capacity to handle the current traffic.

[I.9] Interruption of other services and essential supplies

Types of assets:	Dimensions:
[AUX] auxiliary equipment	1. [D] availability

Description:
Other services or resources on which the operation of the equipment depends, for example, printer paper, toner, coolant, etc.

[I.10] Media degradation

Types of assets:	Dimensions:
[SI] media	1. [D] availability 2. [T_S] accountability of service use 3. [T_D] accountability of data access

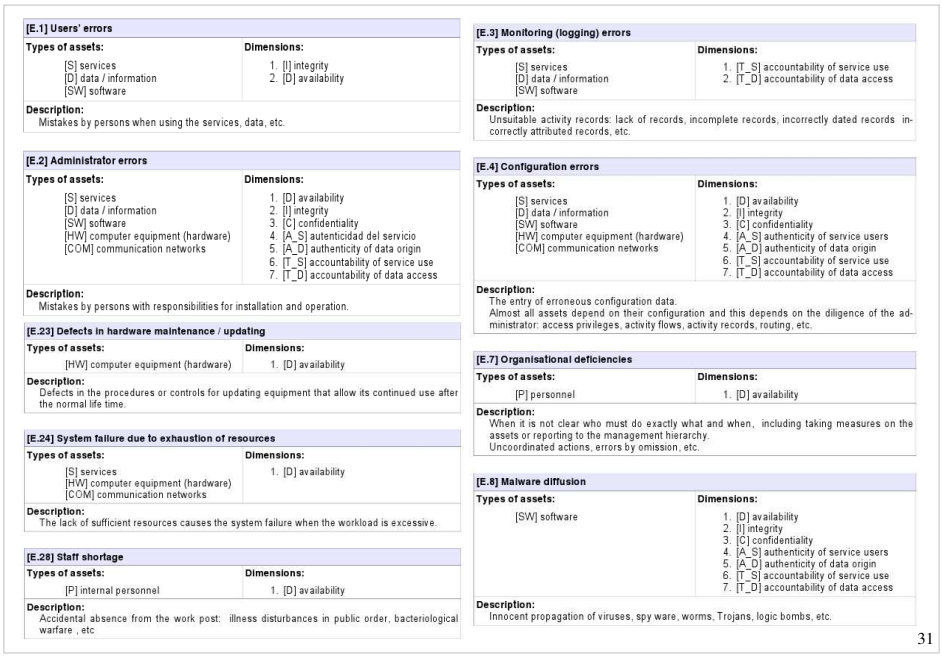
Description:
As the result of the passing of time.

[I.11] Electromagnetic radiation

Types of assets:	Dimensions:
[HW] computer equipment (hardware) [COM] communication networks [L] installations	1. [C] confidentiality

Description:
The fact of making internal data available to third parties by radio.. It is a threat in which the issuer is the passive victim of the attack.
Almost all electrical devices emit radiation to the exterior that can be intercepted by other equipment (radio receivers) causing a leak of information.
This threat is frequently but inaccurately called, a TEMPEST attack ("Transient Electromagnetic Pulse Standard"). Although abusing the original meaning, it is frequent to hear of equipment described as having "TEMPEST protection", meaning that it is designed not to emit electromagnetically anything of interest in case somebody receives it.
This threat does not include emissions for the needs of communication media: wireless networks, microwave links, etc. that may be threatened by interception.

30



[E.1] Users' errors

Types of assets:	Dimensions:
[S] services [D] data / information [SW] software	1. [I] integrity 2. [D] availability

Description:
Mistakes by persons when using the services, data, etc.

[E.2] Administrator errors

Types of assets:	Dimensions:
[S] services [D] data / information [SW] software [HW] computer equipment (hardware) [COM] communication networks	1. [D] availability 2. [I] integrity 3. [C] confidentiality 4. [A_S] autenticidad del servicio 5. [A_D] authenticity of data origin 6. [T_S] accountability of service use 7. [T_D] accountability of data access

Description:
Mistakes by persons with responsibilities for installation and operation.

[E.23] Defects in hardware maintenance / updating

Types of assets:	Dimensions:
[HW] computer equipment (hardware)	1. [D] availability

Description:
Defects in the procedures or controls for updating equipment that allow its continued use after the normal life time.

[E.24] System failure due to exhaustion of resources

Types of assets:	Dimensions:
[S] services [HW] computer equipment (hardware) [COM] communication networks	1. [D] availability

Description:
The lack of sufficient resources causes the system failure when the workload is excessive.

[E.28] Staff shortage

Types of assets:	Dimensions:
[P] internal personnel	1. [D] availability

Description:
Accidental absence from the work post: illness disturbances in public order, bacteriological warfare , etc

[E.3] Monitoring (logging) errors

Types of assets:	Dimensions:
[S] services [D] data / information [SW] software	1. [T_S] accountability of service use 2. [T_D] accountability of data access

Description:
Unsuitable activity records: lack of records, incomplete records, incorrectly dated records incorrectly attributed records, etc.

[E.4] Configuration errors

Types of assets:	Dimensions:
[S] services [D] data / information [SW] software [HW] computer equipment (hardware) [COM] communication networks	1. [D] availability 2. [I] integrity 3. [C] confidentiality 4. [A_S] authenticity of service users 5. [A_D] authenticity of data origin 6. [T_S] accountability of service use 7. [T_D] accountability of data access

Description:
The entry of erroneous configuration data.
Almost all assets depend on their configuration and this depends on the diligence of the administrator: access privileges, activity flows, activity records, routing, etc.

[E.7] Organisational deficiencies

Types of assets:	Dimensions:
[P] personnel	1. [D] availability

Description:
When it is not clear who must do exactly what and when, including taking measures on the assets or reporting to the management hierarchy.
Uncoordinated actions, errors by omission, etc.

[E.8] Malware diffusion

Types of assets:	Dimensions:
[SW] software	1. [D] availability 2. [I] integrity 3. [C] confidentiality 4. [A_S] authenticity of service users 5. [A_D] authenticity of data origin 6. [T_S] accountability of service use 7. [T_D] accountability of data access

Description:
Innocent propagation of viruses, spy ware, worms, Trojans, logic bombs, etc.

31

[E.9] [Re-]routing errors

Types of assets:	Dimensions:
[S] services [SW] software [COM] communication networks	1. [C] confidentiality 2. [I] integrity 3. [A_S] authenticity of service users 4. [T_S] accountability of service use

Description:
The sending of information via a system or network, accidentally. These may be messages between persons using an incorrect route with information passing through or reaching the incorrect place. These could be messages between persons, between processes or between both.
The case of a routing error involving a delivery error, with the information ending up in the hands of someone unexpected is particularly notable.

[E.10] Sequence errors

Types of assets:	Dimensions:
[S] services [SW] software [COM] communication networks	1. [I] integrity

Description:
The accidental alteration of the order of the messages sent.

[E.14] Information leaks

Types of assets:	Dimensions:
[D] data / information [SW] software [COM] communication networks	1. [C] confidentiality

Description:
The information accidentally reaches persons who should not have knowledge of it, without the information itself being altered.

[E.15] Information alteration

Types of assets:	Dimensions:
[D] data / information	1. [I] integrity

Description:
The accidental alteration of the information.
This threat is only identified for data in general, since there are specific threats when information is stored on a computer medium.

[E.16] Entry of incorrect information

Types of assets:	Dimensions:
[D] data / information	1. [I] integrity

Description:
The accidental entry of incorrect information.
This threat is only identified for data in general since there are specific threats when information is stored on a computer medium.

[E.17] Information degradation

Types of assets:	Dimensions:
[D] data / information	1. [I] integrity

Description:
Accidental degradation of the information.
This threat is only identified for data in general since there are specific threats when information is stored on a computer medium.

[E.18] Destruction of information

Types of assets:	Dimensions:
[D] data / information	1. [D] availability

Description:
Accidental loss of information.
This threat is only identified for data in general since there are specific threats when information is stored on a computer medium.

[E.19] Disclosure of information

Types of assets:	Dimensions:
[D] data / information	1. [C] confidentiality

Description:
Disclosure due to indiscretion.
Verbal indiscretion, electronic media, hard copies, etc.

[E.20] Software vulnerabilities

Types of assets:	Dimensions:
[SW] software	1. [I] integrity 2. [D] availability 3. [C] confidentiality

Description:
Defects in the code that cause a defective operation without intention on the part of the user but with consequences to the data integrity or to its capacity to operate.

[E.21] Defects in software maintenance / updating

Types of assets:	Dimensions:
[SW] software	1. [I] integrity 2. [D] availability

Description:
Defects in the procedures or controls for updating the code that allow programs with known defects that have been repaired by the manufacturer to continue to be used.

32

[A.4] Manipulation of the configuration

Types of assets:	Dimensions:
[S] services [D] data / information [SW] software [HW] computer equipment (hardware) [COM] communication networks	1. [I] integrity 2. [C] confidentiality 3. [A_S] authenticity of service users 4. [A_D] authenticity of data origin 5. [T_S] accountability of service use 6. [T_D] accountability of data access 7. [D] availability

Description:
Almost all assets depend on their configuration and this in turn depends on the diligence of the administrator: access privileges, activity flows, activity record, routing, etc.

[A.29] Extortion

Types of assets:	Dimensions:
[P] internal personnel	1. [C] confidentiality 2. [I] integrity 3. [A_S] authenticity of service users 4. [A_D] authenticity of data origin 5. [T_S] accountability of service use 6. [T_D] accountability of data access

Description:
Pressure with threats, on people to oblige them to act in a certain way.

[A.30] Social engineering

Types of assets:	Dimensions:
[P] internal personnel	1. [C] confidentiality 2. [I] integrity 3. [A_S] authenticity of service users 4. [A_D] authenticity of data origin 5. [T_S] accountability of service use 6. [T_D] accountability of data access

Description:
Taking advantage of the good will of some persons to make them carry out activities of interest to a third party.

[A.5] Masquerading of user identity

Types of assets:	Dimensions:
[S] services [SW] software [COM] communication networks	1. [C] confidentiality 2. [A_S] authenticity of service users 3. [A_D] authenticity of data origin 4. [I] integrity

Description:
When attackers manage to appear as authorised users, they enjoy the users' privileges for their own purposes.
This threat may be perpetrated by internal personnel, by persons outside the organisation or by persons contracted temporarily.

[A.6] Abuse of access privileges

Types of assets:	Dimensions:
[S] services [SW] software [HW] computer equipment (hardware) [COM] communication networks	1. [C] confidentiality 2. [I] integrity

Description:
Each user enjoys a level of privileges for a specific purpose. When users abuse their privilege level to carry out tasks that are not their responsibility, there are problems.

[A.7] Misuse

Types of assets:	Dimensions:
[S] services [SW] software [HW] computer equipment (hardware) [COM] communication networks [SI] media [AUX] auxiliary equipment [L] installations	1. [D] availability

Description:
The use of system resources for unplanned purposes, typically of personal interest: games, personal searches on the Internet, personal databases, personal programs, storage of personal data, etc.

[A.8] Malware diffusion

Types of assets:	Dimensions:
[SW] software	1. [D] availability 2. [I] integrity 3. [C] confidentiality 4. [A_S] authenticity of service users 5. [A_D] authenticity of data origin 6. [T_S] accountability of service use 7. [T_D] accountability of data access

Description:
The intentional propagation of viruses, spy ware, worms, trojans, logic bombs, etc.

33

[A.9] [Re-]routing of messages

Types of assets:	Dimensions:
[S] services [SW] software [COM] communication networks	1. [C] confidentiality 2. [I] integrity 3. [A_S] authenticity of service users 4. [T_S] accountability of service use

Description:
The sending of information to an incorrect destination via a system or network, with information passing through or reaching the incorrect place. These may be messages between persons, between processes or between both.
An attacker may force a message to travel through a specific node in the network where it can be intercepted.
Particularly notable is the case in which the routing attack causes a fraudulent delivery, with the information reaching the hands of an unauthorised person.

[A.10] Sequence alteration

Types of assets:	Dimensions:
[S] services [SW] software [COM] communication networks	1. [I] integrity

Description:
The alteration of the order of the messages sent. The idea is that the new order changes the meaning of the group of messages, prejudicing the integrity of the affected data.

[A.11] Unauthorised access

Types of assets:	Dimensions:
[S] services [D] data / information [SW] software [HW] computer equipment (hardware) [COM] communication networks [SI] media [AUX] auxiliary equipment [L] installations	1. [C] confidentiality 2. [I] integrity 3. [A_S] authenticity of service users

Description:
The attacker manages to access the system's resources without authorisation for doing so, typically taking advantage of a failure in the identification and authorisation system.

[A.12] Traffic analysis

Types of assets:	Dimensions:
[COM] communication networks	1. [C] confidentiality

Description:
Without needing to analyse the contents of communications, the attacker can reach conclusions based on the analysis of the origin, destination, volume and frequency of the exchanges.
This is sometimes called "traffic monitoring".

[A.13] Repudiation

Types of assets:	Dimensions:
[S] services	1. [T_S] accountability of service use

Description:
The later rejection of actions or undertakings acquired in the past.
Repudiation of origin: denial of being the sender or origin of a message or communication.
Repudiation of receipt: denial of having received a message or communication.
Repudiation of delivery: denial of having received a message for delivery to others.

[A.14] Eavesdropping

Types of assets:	Dimensions:
[D] data / information [SW] software [HW] computer equipment (hardware) [COM] communication networks	1. [C] confidentiality

Description:
Attackers have access to information that is not theirs, without the information itself being altered.

[A.15] Alteration of information

Types of assets:	Dimensions:
[D] data / information	1. [I] integrity

Description:
Intentional alteration of the information to obtain a benefit or cause damage.
This threat is only identified for data in general since there are specific threats when the data is on a computer medium.

[A.16] Entry of false information

Types of assets:	Dimensions:
[D] data / information	1. [I] integrity

Description:
The deliberate entry of false information to obtain a benefit or cause damage.
This threat is only identified for data in general since there are specific threats when the data is on a computer medium.

[A.17] Corruption of information

Types of assets:	Dimensions:
[D] data / information	1. [I] integrity

Description:
The intentional degradation of the information, to obtain a benefit or cause damage.
This threat is only identified for data in general since there are specific threats when the data is on a computer medium.

34

[A.18] Destruction of information

Types of assets:	Dimensions:
[D] data / information	1. [D] availability

Description:
The intentional deletion of information, to obtain a benefit or cause damage.
This threat is only identified for data in general since there are specific threats when the data is on a computer medium.

[A.19] Disclosure of information

Types of assets:	Dimensions:
[D] data / information	1. [C] confidentiality

Description:
Disclosure of information.

[A.22] Software manipulation

Types of assets:	Dimensions:
[SW] software	1. [C] confidentiality 2. [I] integrity 3. [A_S] authenticity of service users 4. [A_D] authenticity of data origin 5. [T_S] accountability of service use 6. [T_D] accountability of data access

Description:
The intentional alteration of the operation of a program to obtain an indirect benefit when an authorised person uses it.

[A.24] Denial of service

Types of assets:	Dimensions:
[S] services [HW] computer equipment (hardware) [COM] communication networks	1. [D] availability

Description:
The lack of sufficient resources causes the system to fail when the workload is too high.

[A.25] Theft

Types of assets:	Dimensions:
[HW] computer equipment (hardware) [COM] communication networks [SI] media [AUX] auxiliary equipment	1. [D] availability 2. [C] confidentiality

Description:
Theft of equipment directly causes a lack of resources to provide the services, that is, non-availability.
All types of equipment may be affected by theft, the most common being theft of equipment and of information media.
Theft may be carried out by internal personnel, persons outside the organisation or persons contracted temporarily, which sets different degrees of ease for accessing the stolen object and different consequences.
In the case of equipment hosting data, a leak of information may also occur.

[A.26] Destructive attack

Types of assets:	Dimensions:
[HW] computer equipment (hardware) [COM] communication networks [SI] media [AUX] auxiliary equipment [L] installations	1. [D] availability

Description:
Vandalism, terrorism, military action, etc.
This threat may be carried out by internal personnel, by persons outside the organisation or by persons contracted temporarily.

[A.27] Enemy over-run

Types of assets:	Dimensions:
[HW] computer equipment (hardware) [COM] communication networks [SI] media [AUX] auxiliary equipment [L] installations	1. [D] availability 2. [C] confidentiality

Description:
When the premises have been invaded and control is lost over the means of work.

[A.28] Staff shortage

Types of assets:	Dimensions:
[P] internal personnel	1. [D] availability

Description:
Deliberate absence from the work post: such as strikes, labour absenteeism, unjustified absences, the blocking of accesses, etc.

35

STRIDE

- **proposto da Microsoft per analisi delle minacce durante la progettazione di applicazioni software**
- **classificazione dei diversi tipi di minacce**
- **considera la prospettiva dell'attaccante**
- **l'acronimo contiene al suo interno i nomi delle categorie delle minacce**

- **riferimento:**
  - Michael Howard, David Leblanc, "Writing Secure Code", Microsoft Press

36

Le categorie STRIDE

- **Spoofing Identity**
- **Tampering**
- **Repudiation**
- **Information Disclosure**
- **Denial of service**
- **Elevation of Privilege**

37

STRIDE – Spoofing Identity

- **insieme delle minacce che permettono ad un attaccante di interagire con il sistema utilizzando un'altra identità**
- **esempio:**
  - un server di phising che pretende di essere il server della mia banca

38

STRIDE – Tampering

- **insieme delle minacce che permettono di modificare in modo fraudolento:**
  - dati
  - codice delle applicazioni
- **esempio:**
  - un attaccante sfruttando un bug software riesce a cambiare il codice di un'applicazione per aprire una backdoor nel sistema

39

STRIDE – Repudiation

- **insieme delle minacce che permettono ad un attaccante di negare di aver compiuto un'azione sul sistema**
- **esempio:**
  - un utente compie un'azione illegale sul sistema e il sistema non è in grado di rilevare l'azione o identificare l'utente

40

STRIDE – Information Disclosure

- **insieme delle minacce che provocano l'esposizione di informazioni ad utenti/individui a cui non è consentito l'accesso in lettura/scrittura**
- **esempi:**
  - un utente legge un file per il quale non ha ricevuto i diritti di lettura
  - un attaccante legge i dati in transito sulla rete

41

STRIDE – Denial of Service

- **insieme delle minacce che permettono di negare o degradare la fornitura di un servizio**
- **esempio:**
  - un attaccante invia molti pacchetti al fine di intasare la banda di un server il quale non potrà essere contattato e/o fornire i suoi servizi agli utenti

42

STRIDE – Elevation of Privilege

- **insieme delle minacce che permettono ad un utente di ottenere privilegi non previsti per il suo ruolo**
- **esempio:**
  - un utente anonimo sfruttare un bug software per ottenere i privilegi di amministratore

43

STRIDE: relazione con i beni

- **relazione tra categorie STRIDE e gli elementi di un modello DFD:**

categorie STRIDE / elementi DFD	S	T	R	I	D	E
agenti esterni	X		X			
flusso di dati		X		X	X	
archivi		X	X*	X	X	
processi	X	X	X	X	X	X

cfr. M.Howard, S.Lipner, The Security Development Lifecycle, Microsoft Press, pp. 119

* se l'archivio contiene dati di audit o di logging, un attaccante potrebbe manipolarli per nascondere le sue tracce

44

STRIDE: critiche

- **STRIDE non è una tassonomia:**
  - molte categorie sono correlate
  - es. escalation of privilege tipicamente implica spoofing e loss of non-repudiation, e può implicare tampering, information disclosure e denial of service
  - impedendo la definizione di un processo di identificazione pienamente formale
- **un problema generale, non solo di STRIDE**

cfr. http://blogs.msdn.com/david_leblanc/archive/2007/08/13/dreadful.aspx

45

Nota sulla formalizzazione

- **perché è desiderabile formalizzare i processi dell'analisi dei rischi?**
  - per poter automatizzare la loro implementazione e/o verifica
- **da qui lo sforzo nel definire**
  - tassonomie e ontologie
  - modelli e rappresentazioni
  - algoritmi e processi formali
- **da affiancare alle metodologie più o meno empiriche usate finora**

46

Relazioni causa - effetto

- **dato che un incidente è un insieme di eventi, è opportuno studiare le relazioni tra minacce:**
  - in genere di causa - effetto
  - tra tipo di sorgente e beni coinvolti
  - tra modalità e effetti
  - tra gli effetti di un incidente e ulteriori minacce

47

Relazioni causa - effetto

- **utili per:**
  - calcolo della valorizzazione delle minacce
  - computo dell'impatto
  - selezione dei controlli
  - far comprendere l'effettiva concretezza dei risultati dell'analisi dei rischi

48

Relazioni causa - effetto

- **concetto della 'superficie di attacco' (attack surface)**
- **modellare le relazioni tra minacce è propedeutico per**
  - la creazione di modelli strutturati delle minacce
  - l'automazione delle procedure di identificazione e valorizzazione delle minacce
- **un aspetto sviluppato solo nelle metodologie più moderne (oggetto di ricerca)**

49

Modellazione delle relazioni tra minacce

- **molte metodologie sono usate nell'analisi dei fault:**
  - fault tree analysis (FTA)
  - event tree analysis (ETA)
  - failure mode and effects analysis (FMEA/FMECA)
  - ...
- **meno consolidati i metodi per la sicurezza (argomento di ricerca):**
  - attack tree/graph
  - varianti: privilege graph, exploit graph

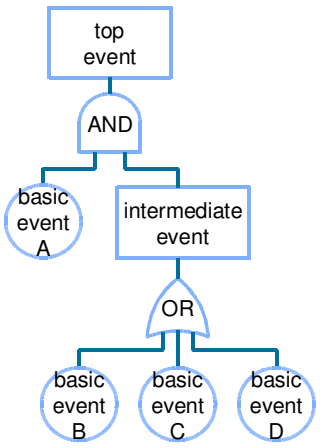
50

Fault Tree Analysis

- **tecnica nata nel 1962 presso i Bell Labs e perfezionata da Boing**
- **usata per sistemi di controllo missilistici, impianti nucleari e petrolchimici**
- **modello per analisi backward (deduttiva)**
  - costruisce diagrammi di blocchi logici che rappresentano lo stato del sistema in termini degli stati dei suoi componenti

51

Fautl Tree Analysis



52

Fautl Tree Analysis

1. **parto da un evento indesiderato (top event)**
2. **lo inserisco come nodo radice in un albero logico**
3. **determino gli eventi che ne costituiscono le cause immediate, necessarie e sufficienti**
4. **collego i nuovi eventi alla radice via operatori logici che hanno come input una combinazione delle cause e output il top event**
5. **itero sui nuovi eventi fino ad individuare deli eventi elementari o errori umani (basic events)**

53

Fault tree: simboli

Nome	*Simbolo*	*Significato*
evento di base (Basic Event)		evento iniziatore di base che non richiede ulteriore sviluppo
evento non sviluppato (Undeveloped Event)		BE non indagato ulteriormente
evento condizionante (Conditioning Event)		evento che indica una qualsiasi condizione o restrizione da applicare ad una porta logica (Priority AND e INHIBIT).
evento esterno (House Event)		BE esterno ai componenti del sistema, quale può essere, ad esempio un incendio di un edificio, un'errata manutenzione…

Nome	*Simbolo*	*Significato*
TRANSFER IN		Denota l'esistenza di un sotto-albero che parte proprio da questo punto, ma che è sviluppato altrove, sotto un simbolo di Trasfer_OUT
TRANSFER OUT		È un collegamento ad un simbolo di Trasfer_IN e indica che il sotto-albero (figlio) che si sviluppa al di sotto di questo simbolo è in realtà una porzione di un albero più esteso (padre).

Nome	*Simbolo*	*Significato*
AND		L'evento in output accade se e solo se tutti gli eventi in input accadono simultaneamente
OR		Uno degli eventi in input produce l'evento in output indipendentemente dall'occorrenza degli altri
EXOR		L'evento in output accade se e solo se si verifica unicamente uno degli eventi in input.
INHIBIT		Utilizzata con un evento condizionante che, se non verificato, blocca la propagazione dell'evento in input
PRIORITY AND		L'evento in output accade solo se tutti gli eventi accadono in una sequenza specifica
COMBINATION		L'evento in output accade solo se n eventi in input accadono

NASA, Fault Tree Handbook with Aerospace Application (Agosto 2002)
http://www.hq.nasa.gov/office/codeq/doctree/fthb.pdf

W. Vesely et al., Fault Tree Handbook, NUREG-0492, Nuclear Regulatory Commission (1981)
http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0492/sr0492.pdf

54

Event Tree Analysis

- **metodo di analisi che mostra tutti i possibili esiti risultanti dallo scatenarsi un evento (initiating event)**
- **valuta le conseguenze lungo una serie di possibili cammini, ad ognuno dei quali e assegnata una particolare probabilità di occorrenza**
- **modello per analisi forward (induttiva)**

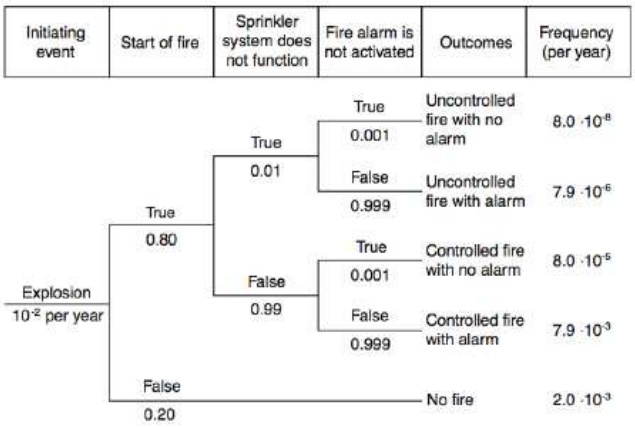
57

Event Tree Analysis

- **Nell'albero degli eventi si considerano gli effetti che i vari sistemi di sicurezza (barrier, barriere) generano in conseguenza dell'evento iniziale**
- **le barriere relative ad ogni evento analizzato sono elencate nell'ordine di attivazione**
- **le conseguenze sono rappresentate in termini di danneggiamento (ok/danno parziale/distruzione totale) dei componeti del sistema**

58

Event Tree Analysis



Rausand, M. e A. Høyland: System Reliability Theory; Models, Statistical Methods and Applications Wiley, New York, 2004.

59

Event Tree Analysis

1. **identificare e definire un evento iniziatore rilevante;**
2. **identificare le barriere progettate per contrastare questo evento indesiderato;**
3. **costruire l'event tree;**
4. **descrivere le (potenziali) sequenze di incidenti risultanti;**
5. **determinare la frequenza dell'evento indesiderato e le probabilità (condizionali) dei rami nell'event tree;**
6. **calcolare le probabilità / frequenze per le conseguenze (esiti) identificate.**

60

Failure Mode and Effects Analysis

- **mira ad analizzare tutti i potenziali failure mode di un sistema per determinarne gli effetti sulla funzionalità**
- **FMECA (Failure Mode, Effects, and Criticality Analysis) estende FMEA con l'analisi delle criticità dei failure mode**
  - probabilità di occorrenza (P)
  - gravità (G), impatto del failure sulla sicurezza e le prestazioni funzionali;
  - rilevabilità (R), quanto il failure può essere individuato nel processo;
  - criticità (C), o indice RPN (Risk Priority Number) C = P * G * R

62

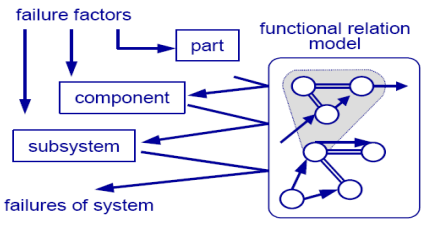
Le tre fasi FMEA/FMECA

- **fase preliminare:**
  - costruzione di un diagramma della struttura funzionale del sistema
- **analisi qualitativa:**
  - definizione dei failure mode per singolo elemento
  - identificazione delle possibili cause
  - analisi dell'effetto locale e globale dei failure mode
- **analisi quantitativa:**
  - stima della probabilità di occorenza per failure mode
  - valutazione della criticità (RPN)
  - identificazione delle azioni correttive

63

FMEA/FMECA

- **www.weibull.com/mil_std/mil_std_1629a.pdf**



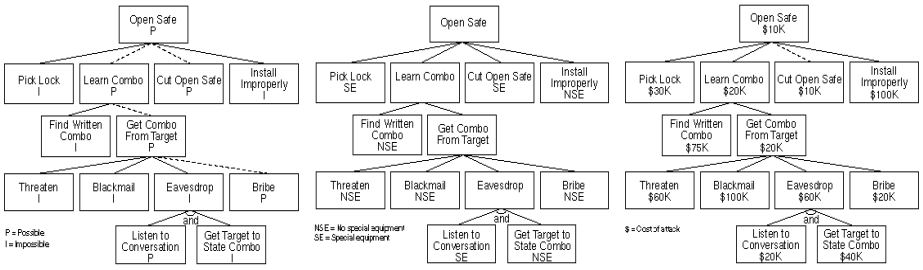
Process	Pharmacy	Dispense	O.R.	Transfer	Sterile field	Administer	Patient
Potential failure modes	Look-alike drugs Multiple concentrations	Wrong drug Wrong concentration		Switched drugs Contamination		Wrong drug Wrong dose	
Potential effect on patient	8	8		10		10	
Frequency of failure mode	7	3		2		3	

fonte: anonimo

64

Attack tree/graph

- **proposti da Bruce Schneier**
  - www.schneier.com/paper-attacktrees-ddj-ft.html



fonte: www.scheneier.com

65

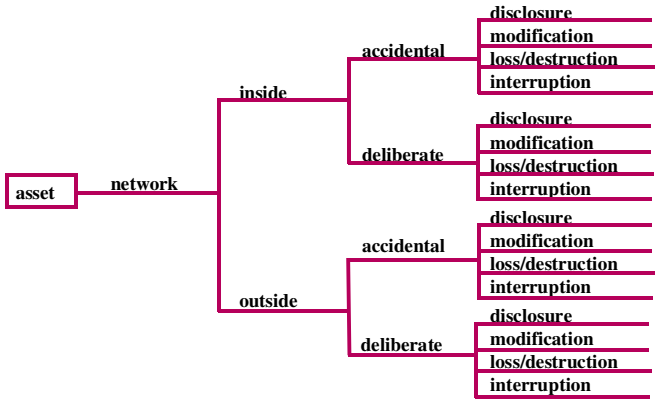
Attack tree/graph

- **usati da alcune metodologie recenti**
  - Microsoft threat modelling
  - Octave

66

Octave: template per attack tree

Human Actors - Network Access

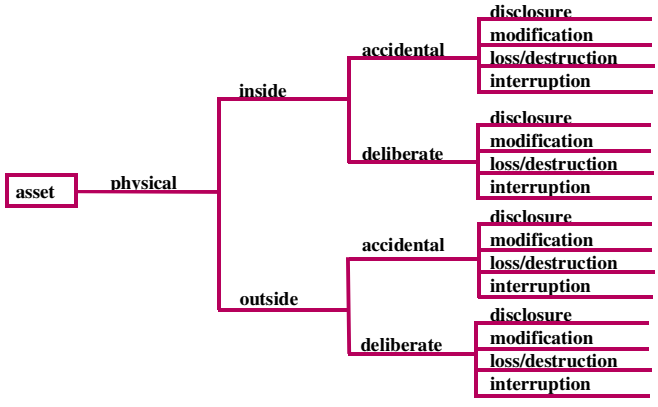


asset access actor motive outcome fonte: OCTAVE

67

Octave: template per attack tree

Human Actors - Physical Access

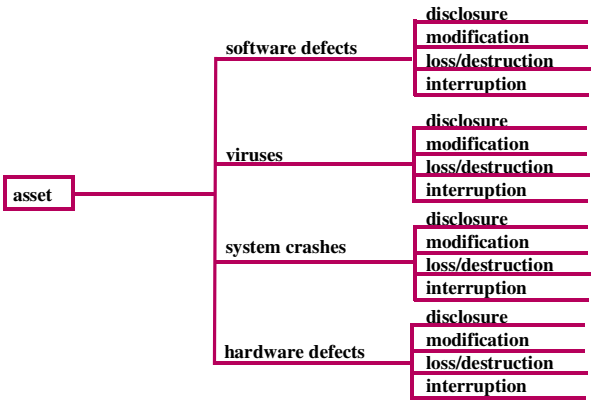


asset access actor motive outcome fonte: OCTAVE

68

Octave: template per attack tree

System Problems

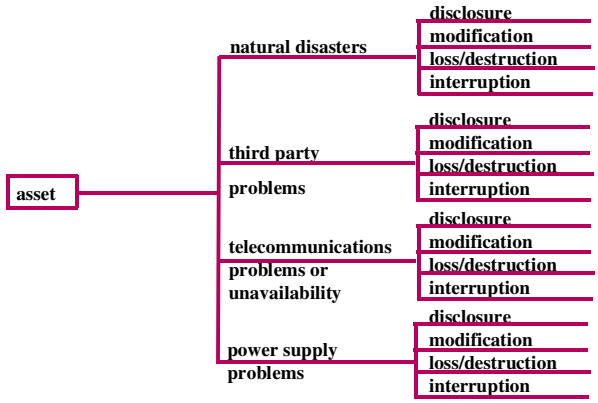


fonte: OCTAVE

69

Octave: template per attack tree

Other Problems



fonte: OCTAVE

70

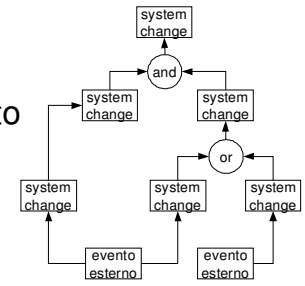
Modello strutturato delle minacce: esempio

- **grafo direzionato**
  - nodi =
    - possibili cambiamenti nel modello strutturato del sistema (riguardanti beni, relazioni, valori)
    - + operatori logici (AND, OR, ...)
    - + possibili eventi scatenanti esterni al modello (es. alluvione, ...)
  - archi = relazioni di causalità

71

Modello strutturato delle minacce: esempio

- **in pratica, una minaccia è una o più deviazioni potenziali da quanto prescritto dal modello strutturato del sistema**
- **questo modello può essere costruito a partire da**
  - dipendenze descritte dal modello strutturato del sistema
  - libreria di minacce per categoria di elemento del modello strutturato



72

Analogia medica

- **diagnosi:**
  - le possibili cause alternative (OR) e concause (AND) di una situazione di danno (incidente)
- **prognosi:**
  - gli effetti stimati, a breve e lungo termine
- **sintomi:**
  - eventi osservabili che caratterizzano la situazione di danno
    - utili a pianificare processi di monitoraggio in caso non si possa prevenire completamente la minaccia

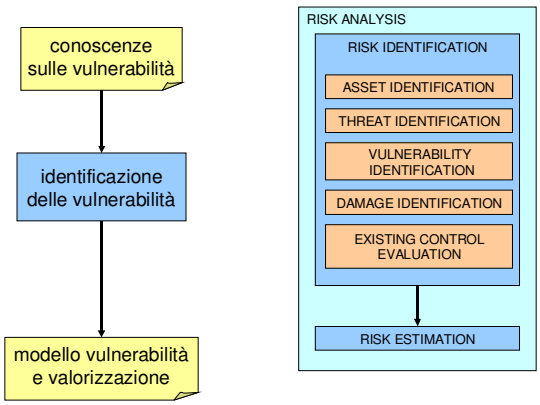
73

2.1.3. Identificazione delle vulnerabilità

- **vulnerabilità:**
  - una debolezza che può essere sfruttata da una fonte di minaccia per danneggiare il sistema e i suoi beni (ISO 27005)
  - una mancanza o debolezza, nelle procedure di scurezza, nel progetto, implementazione o controlli del sistema, che può essere esercitata e causare una violazione di sicurezza (SP 800-30)
- **in effetti il processo consiste in due passi:**
  - identificare le vulnerabilità
  - per ognuna valutare il livello di debolezza (facilità nell'essere esercitata)

74

2.1.3. Identificazione delle vulnerabilità



75

Tipi di vulnerabilità

- **le vulnerabilità possono trovarsi a tutti i livelli:**
  - organizzativo (organization)
  - nei processi e procedure (process and procedures)
  - nella gestione (management)
  - nel personale (personnel)
  - nell'ambiente fisico (physical environment)
  - nella configurazione dei sistemi IT (ICT configuration)
  - nell'hardware, software, e dispositivi di comunicazione (equipment)
  - ...

76

Tipi di vulnerabilità

- **dipendono fortemente dalle tecnologie usate e dalla fase di sviluppo del sistema sotto analisi**
  - per questo motivo è intrinsecamente difficile costruire e mantenere una tassonomia completa delle vulnerabilità
- **in pratica, vengono identificate per negazione:**
  - mancata applicazione di una best practice
    - es. mancanza di un controllo
  - efficacia non completa di una best practice
    - un segreto conservato su un qualche supporto non è mai porotetto al 100%

77

Best practice e checklist

- **codici di condotta**
- **esistono best practice a tutti i livelli:**
  - organizzativo
  - progetto e gestione di processi e procedure
  - progetto e sviluppo software
  - configurazione dei dispositivi hardware e software
  - configurazione dei controlli di sicurezza
  - protezione ambiente fisico
  - gestione del personale
  - ...

78

Tipi di best practice: esempio

Security Area	Security Criteria
Management Security	• Assignment of responsibilities • Continuity of support • Incident response capability • Periodic review of security controls • Personnel clearance and background investigations • Risk assessment • Security and technical training • Separation of duties • System authorization and reauthorization • System or application security plan
Operational Security	• Control of air-borne contaminants (smoke, dust, chemicals) • Controls to ensure the quality of the electrical power supply • Data media access and disposal • External data distribution and labeling • Facility protection (e.g., computer room, data center, office) • Humidity control • Temperature control • Workstations, laptops, and stand-alone personal computers
Technical Security	• Communications (e.g., dial-in, system interconnection, routers) • Cryptography • Discretionary access control • Identification and authentication • Intrusion detection • Object reuse • System audit

fonte:
SP 800-30,
pp 18-19

79

Best practice e checklist

- **una checklist contiene una lista di verifiche da eesmguire per stabilire la conformità ad un insieme standard di best practice:**
  - per uno specifico business
  - per una specifica normativa
  - per uno specifico processo
  - per una specifica organizzazione
  - per uno specifico tipo di sistema
  - per specifici sottosistemi e componenti

80

Checklist: esempi

- **di configurazione:**
  - identificano i parametri sensibili nella configurazione di specifici componenti del sistema
  - suggeriscono valori appropriati
- **per sviluppo software:**
  - indicazioni per la scrittura di codice sicuro

81

Conoscenza delle vulnerabilità

- **tipi di vulnerabilità rilevanti e metodi di identificazione dipendono dalla fase di sviluppo**
  - in fase di progetto concentrarsi su:
    - procedure di sicurezza pianificate, requisiti di sistema, analisi di sicurezza fornite da produttori e sviluppatori (es. white papers)
  - durante l'implementazione concentrarsi su:
    - funzionalità di sicurezza specificate nel progetto, risultati dei test di certificazione e valutazione
  - in produzione concentrarsi su:
    - funzionalità del sistema IT incluse le funzionalità di sicurezza, controlli tecnici e procedurali

82

Conoscenza delle vulnerabilità

- **la costruzione/aggiornamento delle informazioni sulle vulnerabilità può avvalersi di:**
  - dumentazione interna
  - checklist
  - cataloghi di vulnerabilità
  - strumenti automatici

83

Documentazione

- **risultati di precedenti analisi dei rischi sul sistema**
- **rapporti su incidenti e anomalie**
- **rapporti di ispezione e certificazione**
- **risultati di test e valutazioni di sicurezza**

84

Test e valutazioni di sicurezza

- **(security test and evaluation, STE)**
- **tipicamente su specifici componenti/sottosistemi**
- **lo scopo è verificare che i requisiti di sicurezza siano soddisfatti dai controlli esistenti e pianificati**
- **in formato tabellare, con ogni requisito accompagnato da una spiegazione di come è soddisfatto o meno nel progetto e/o implementazione**

85

Test e valutazioni di sicurezza

- **metodi generalmente basati su checklist**
- **possono avvalersi di strumenti automatici**
- **possono prevedere lo sviluppo e esecuzione di piani di test (es. script e procedure di test, e risultati attesi)**
- **penetration testing**
  - servizio fornito da aziende specializzate
  - costoso

86

Test e valutazioni di sicurezza

- **guide:**
  - NIST SP 800-115, Technical Guide to Information Security Testing and Assessment
    - NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems
  - guide OWASP: Testing Guide, Code Review, Application Security Verification Standard
  - OCTAVE include delle linee guida

87

Strumenti automatici

- **strumenti di scansione delle vulnerabilità**
  - basati su cheklist e catalogi di vulnerabilità
  - es. Nessus, OVAL interpreter
- **strumenti di analisi del codice sorgente**
- **lo sviluppo di strumenti automatici sta ricevendo una crescente attenzione sia dalla ricerca sia dai produttori**

88

Cataloghi di vulnerabilità

- **identificano debolezze in specifici componenti**
  - in particolare software
- **in genere includono informazioni su:**
  - modalità di sfruttamento della vulnerabilità
  - descrizione (+ o - completa) degli effetti
  - riferimenti a informazioni per rimuovere/mitigare la vulnerabilità (es. patch, hot fix, service pack)
- **spesso organizzati in categorie**
- **nel caso di sviluppo software corrispondono ai cataloghi di errori comuni**

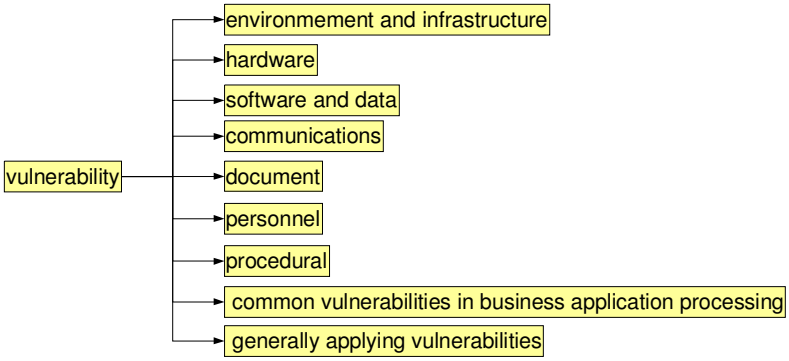
89

Fonti per checklist e cataloghi vulnerabilità

- **siti dei produttori**
  - es. Microsoft Technet, Red Hat, IBM X-Force, ...
- **organismi di Computer Emergency Response**
  - es. CERT.org, US-CERT.gov, GovCERT.it
- **organismi di standardizzazione**
  - MITRE.org (CVE, OVAL)
- **organizzazioni di sensibilizzazione**
  - es. OWASP.org, SANS.org
- **molti offrono newsletter e altri feed per aggiornamento e allarme**

90

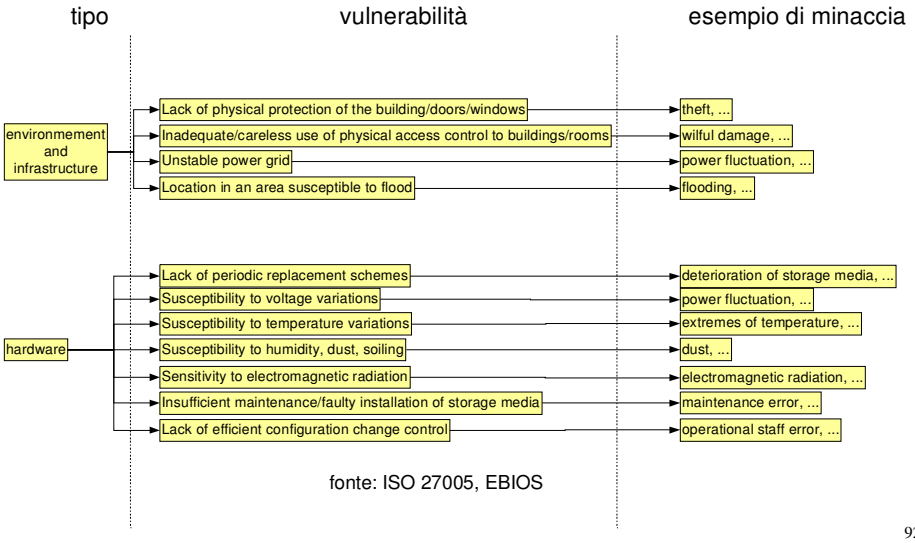
Catalogo vulnerabilità: esempio



fonte: ISO 27005, EBIOS

91

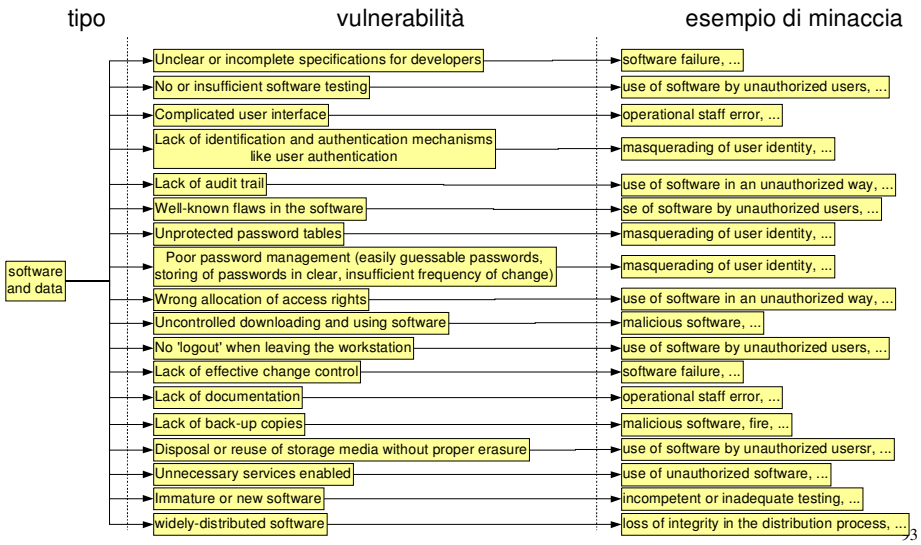
Catalogo vulnerabilità: esempio



fonte: ISO 27005, EBIOS

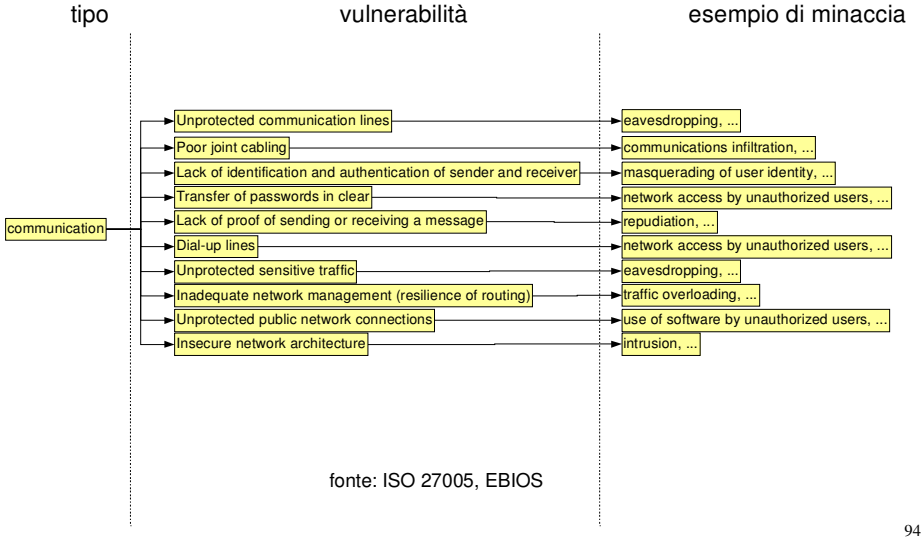
92

Catalogo vulnerabilità: esempio



93

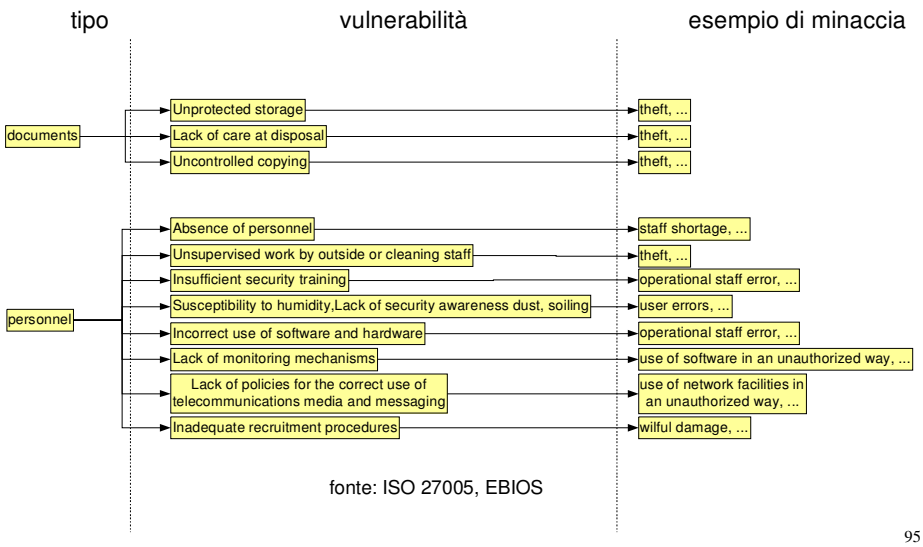
Catalogo vulnerabilità: esempio



fonte: ISO 27005, EBIOS

94

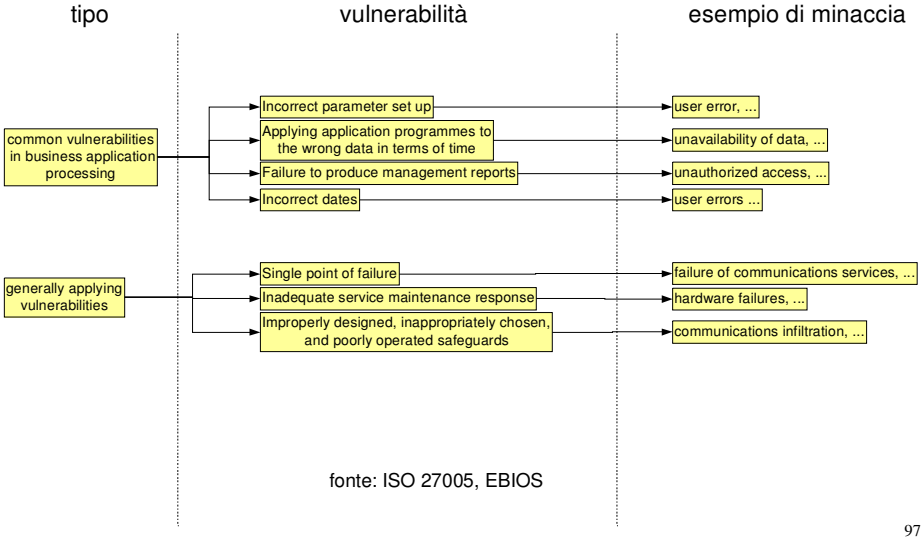
Catalogo vulnerabilità: esempio



fonte: ISO 27005, EBIOS

95

Catalogo vulnerabilità: esempio



fonte: ISO 27005, EBIOS

97

Cataloghi di vulnerabilità software: esempi

- **US CERT (us-cert.gov)**
  - base dati di bollettini di sicurezza e vulnerabilità per componenti software
- **OWASP (www.owasp.org)**
  - TOP 10: le 10 vulnerabilità applicative più critiche
  - catalogo vulnerabilità, attacchi, ... sul sito (wiki)
- **SANS (www.sans.org)**
  - TOP 20 Vulnerabilities (annuale)
  - CWE/SANS TOP 25 Most Dangerous Programming Errors

98

National Vulnerability Database (NVD)

- **nvd.nist.gov**
- **base dati del governo USA per informazioni standard per gestione vulnerabilità**
  - per standardizzazione e automatizzazione di processi di gestione vulnerabilità, misaure di sicurezza, verifiche di conformità
- **consultabile online o scaricabile in formato XML**

99

NVD: contenuti

- **include:**
  - vulnerabilità software
  - errori di configurazione
  - checklist di configurazione
  - script per valutazioni di sicurezza
- **basato su un insieme di standard pubblici sviluppati da NIST e MITRE**

100

NVD: vulnerabilità

- **vulnerabilità software:**
  - breve descrizione testuale
  - identificativo univoco (CVE)
  - descrizione di modalità e conseguenze (CVSS)
  - software e versioni vulnerabili (CPE)
  - classificazione (CWE)
  - riferimenti esterni ad avvisi, soluzioni (patch, hot fix, service pack), e strumenti automatici (CERT, siti produttori, OVAL) per identificare/rimuovere/mitigare la vulnerabilità

101

NVD: altri contenuti

- **errori di configurazione:**
  - in via di sviluppo
  - descrizione basata sullo standard Common Configuration Enumeration (CCE) di MITRE
- **checklist di configurazione:**
  - riferimenti esterni
  - in fase di sviluppo l'uso dello standard Extensible Configuration Checklist Description Format (XCCDF) di NIST
- **script per valutazioni di sicurezza**
  - query OVAL

102

NVD: esempio

Original release date:12/10/2008
Last revised:03/04/2009
Source: US-CERT/NIST
Static Link: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4032

Overview:
Microsoft Office SharePoint Server 2007 Gold and SP1 and Microsoft Search Server 2008 do not properly perform authentication and authorization for administrative functions, which allows ...

Impact:
CVSS Severity (version 2.0):
CVSS v2 Base Score:7.5 (HIGH) (AV:N/AC:L/Au:N/C:P/I:P/A:P) (legend)
Impact Subscore: 6.4
Exploitability Subscore: 10.0
CVSS Version 2 Metrics:
Access Vector: Network exploitable
Access Complexity: Low
Authentication: Not required to exploit
Impact Type:Provides unauthorized access, Allows partial confidentiality, integrity, and availability violation; Allows unauthorized disclosure of information; Allows disruption of service

...

103

NVD: esmpio

...

References to Advisories, Solutions, and Tools:
US-CERT Technical Alert: TA08-344A
Name: TA08-344A
Hyperlink:http://www.us-cert.gov/cas/techalerts/TA08-344A.html
External Source: SECTRACK
Name: 1021367
Hyperlink:http://www.securitytracker.com/id?1021367
External Source: MS
Name: MS08-077
Type: Advisory
Hyperlink:http://www.microsoft.com/technet/security/Bulletin/MS08-077.mspx
External Source: VUPEN
Name: ADV-2008-3389
Hyperlink:http://www.frsirt.com/english/advisories/2008/3389
External Source: SECUNIA
Name: 33063
Hyperlink:http://secunia.com/advisories/33063
External Source: OVAL
Name: oval:org.mitre.oval:def:5774
Hyperlink:http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5774

104

NVD: esempio

...

Vulnerable software and versions
Configuration 1
OR
* cpe:/a:microsoft:office_sharepoint_server:2007:sp1:x32
* cpe:/a:microsoft:office_sharepoint_server:2007:sp1:x64
* cpe:/a:microsoft:office_sharepoint_server:2007::x32
* cpe:/a:microsoft:office_sharepoint_server:2007::x64
* cpe:/a:microsoft:search_server:2008::x32
* cpe:/a:microsoft:search_server:2008::x64
* Denotes Vulnerable Software

Technical Details
Vulnerability Type (View All)

* Authentication Issues (CWE-287)

CVE Standard Vulnerability Entry:http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4032

105

Common Vulnerability and Exposure(CVE)

- **cve.mitre.org**
- **dizionario di identificativi univoci e standard per vulnerabilità e esposizioni note**
- **utile per interoperabilità tra diversi strumenti, basi dati, procedure**
- **diffusissimo:**
  - gestione vulnerabilità e patch
  - avvisi e bollettini di sicurezza
  - intrusion detection
  - database vulnerabilità
- **disponibile in vari formati (online, XML, HTML, TXT ...)**

106

Common Vulnerability and Exposure(CVE)

- **vulnerabilità = un errore nel software che può essere direttamente usato da un hacker per ottenere accesso a un sistema o rete, in particolare che:**
  - permette di eseguire comandi come un'altro utente
  - permette l'accesso a dati in contrasto con le restrizioni di accesso definitee pr quei dati
  - permette di impersonare un'altra entità
  - permette di condurre una privazione di servizio

107

Common Vulnerability and Exposure(CVE)

- **esempi di vulnerabiltà:**
  - phf (remote command execution as user "nobody")
  - rpc.ttdbserverd (remote command execution as root)
  - world-writeable password file (modification of system-critical data)
  - default password (remote command execution or other access)
  - denial of service problems that allow an attacker to cause a Blue Screen of Death
  - smurf (denial of service by flooding a network)

108

Common Vulnerability and Exposure(CVE)

- **esposizione = configurazione di sistema o errore nel software che non permette una compromissione, ma può essere componente di un attacco, e viola una ragionevole politica di sicurezza, in particolare che:**
  - permette di condurre attività di raccolta informazioni
  - permette di nascondere attività
  - include una funzione che si comporta correttamnte, ma che può essere facilmente compromessa
  - è un punto di accesso primario usabile per tentare di acqusire accesso a sistemi e dati
  - è considerato un problema rispetto a qualche ragionevole politica di sicurezza

109

Common Vulnerability and Exposure(CVE)

- **esempi di esposizioni:**
  - running services such as finger (useful for information gathering, though it works as advertised)
  - inappropriate settings for Windows NT auditing policies (where "inappropriate" is enterprise-specific)
  - running services that are common attack points (e.g., HTTP, FTP, or SMTP)
  - use of applications or services that can be successfully attacked by brute force methods (e.g., use of trivially broken encryption, or a small key space)

110

CVE: esempio

Name: CVE-1999-0002

Description:
Buffer overflow in NFS mountd gives root access to remote attackers, mostly in Linux systems. Status: Entry
Reference: SGI:19981006-01-I
Reference: URL:ftp://patches.sgi.com/support/free/security/advisories/19981006-01-I
Reference: CERT:CA-98.12.mountd
Reference: CIAC:J-006
Reference: URL:http://www.ciac.org/ciac/bulletins/j-006.shtml
Reference: BID:121
Reference: URL:http://www.securityfocus.com/bid/121
Reference: XF:linux-mountd-bo

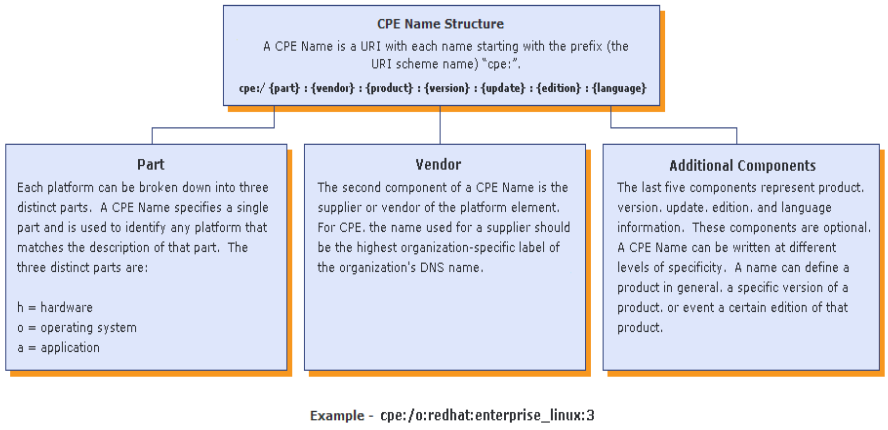
111

Common Platform Enumeration (CPE)

- **cpe.mitre.org**
- **un formato strutturato per attribuire nomi univoci a sistemi, piattaforme e package IT**
  - basato su Uniform Resource Identifiers (URI)
- **un linguaggio per descrivere piattaforme complesse**
  - es. applicazione + OS + hardware
- **procedura per confrontare nomi contro un sistema**
  - include un formato per associare a un nome dei test di confronto (es. stringhe, OVAL)
- **un dizionario ufficiale (in formato XML)**
  - http://nvd.nist.gov/cpe.cfm

112

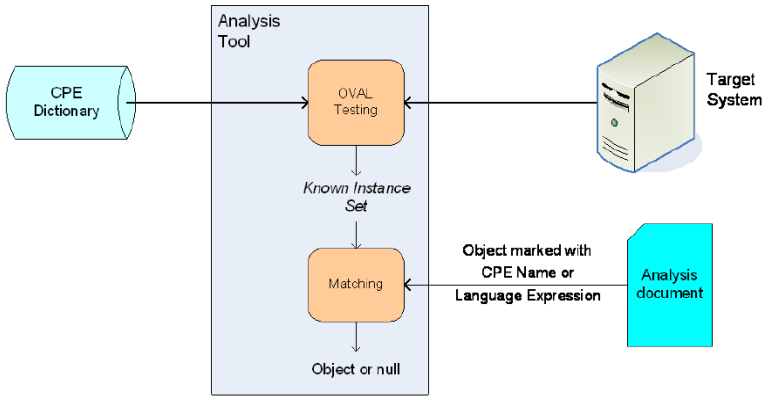
CPE: formato dei nomi



fonte: MITRE

113

CPE: procedura di confronto



fonte: MITRE

114

Common Weakness Enumeration (CWE)

- **cwe.mitre.org**
- **classifica le debolezze software note**
  - secondo varie categorizzazione di uso comune
  - secondo una specifica tassonomia proposta sulla base di un modello dinamico delle vulnerabilità software
    - http://cwe.mitre.org/documents/vulnerability_theory/intro.html
- **in fase di studio un sistema di valutazione**
  - CWSS - Common Weakness Scoring System

115

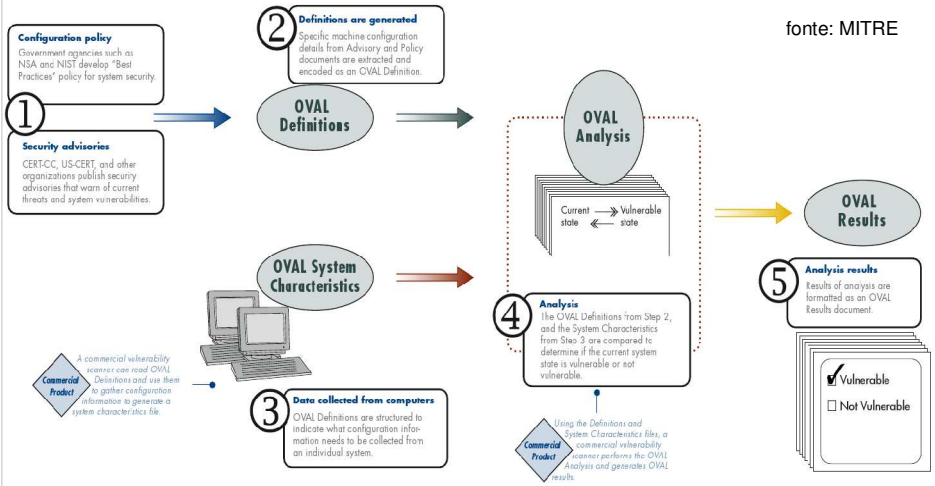
Open Vulnerability and Assessment Language (OVAL)

- **oval.mitre.org**
- **linguaggio XML**
- **rappresenta tre tipi di informazioni utili al processo di identificazione delle vulnerabilità:**
  - informazioni sulla configurazione dei sistemi
  - analisi del sistema alla ricerca di specifici stati (vulnerabilità, misconfigurazioni, patch, ...)
  - presentazione dei risultati della valutazione
- **MITRE fornisce un tool open source per analisi:**
  - OVAL Interpreter http://sourceforge.net/projects/ovaldi/

117

OVAL: funzionamento

fonte: MITRE



118

OVAL: componenti del linguaggio

OVAL System Characteristics schema:

- **schema XML per rappresentare la configurazione di un computer (parametri OS, software installato, parametri applicazioni)**
- **fornisce un database di caratteristiche da confrontare con le definizioni OVAL per identificare uno specifico stato del sistema**
- **utile anche per scambio di informazioni tra tool**
  - supportato da alcuni tool commerciali

119

OVAL: componenti del linguaggio

OVAL Definition schema:

- **schema XML per decrivere test automatici per identificare uno specifico stato di un computer (vulnerabilità, conformità, ...)**
- **due parti: core schema + schemi per specifici OS (Windows, UNIX, ...) o applicazioni (Apache)**

120

OVAL: componenti del linguaggio

- **4 classi di definizioni:**
  - Vulnerability: condizioni che devono esistere su un computer perché una vulnerabiltà sia presente
  - Patch: condizioni per determinare se una patch è adatta a un computer
  - Inventory: condizioni per determinare se un software è installato su un computer on a computer
  - Compliance: condizioni che determinano la cponformità di un computer con una politica o direttiva di configurazione

121

OVAL: componenti del linguaggio

OVAL Results Schema:

- **schema XML per archiviare i risultati della valutazione di una sistema (i.e. lo stato di configurazione del sistema confrontato con un insieme di definizioni OVAL)**
- **utile per scambio di informazioni tra tool**
- **la differenza rispetto al Definition schema è che permette di rappresentare i dati di sistema usati nella valutazione delle definizioni e il risultato finale**

122

OVAL: esempio

```
<oval_definitions ...>
<definitions>
  <definition id="oval:org.mitre.oval:def:5774" version="1" class="vulnerability">
      <metadata>
            <title>Access Control Vulnerability</title>
            <affected family="windows">
                  <platform>Microsoft Windows XP</platform>
                  <platform>Microsoft Windows Server 2008</platform>
                  <product>Microsoft Office SharePoint Server 2007</product>
                  <product>Microsoft Search Server 2008</product>
            </affected>
            <reference source="CVE" ref_id="CVE-2008-4032" ref_url="http://cve.mitre.org/cgi-bin/cvename.cgi?
              name=CVE-2008-4032"/>
            <description>
              Microsoft Office SharePoint Server 2007 Gold and SP1 and Microsoft Search Server 2008 do not properly
              perform authentication and authorization for administrative functions, which allows ...
            </description>
      </metadata>
      <criteria operator="AND">
            <extend_definition comment="Microsoft Office SharePoint Server 2007 is installed."
              definition_ref="oval:org.mitre.oval:def:2313"/>
            <criterion comment="the version of Mssdmn.exe is less than 12.0.6031.5000"
              test_ref="oval:org.mitre.oval:tst:9391"/>
      </criteria>
  </definition>
                                                                ...
```

123

OVAL: esempio

```
                                                                ...

  <definition id="oval:org.mitre.oval:def:2313" version="2" class="inventory">
      <metadata>
            <title>Microsoft Office SharePoint Server 2007 is installed.</title>
            <affected family="windows">
                  <platform>Microsoft Windows XP</platform>
                  <platform>Microsoft Windows Server 2003</platform>
                  <platform>Microsoft Windows Vista</platform>
            </affected>
            <reference source="CPE" ref_id="cpe:/a:microsoft:sharepoint:2007"/>
            <description>Microsoft Office SharePoint Server 2007 is installed.</description>
      </metadata>
      <criteria>
            <criterion comment="SharePoint Server 2007 is installed." test_ref="oval:org.mitre.oval:tst:4279"/>
      </criteria>
</definitions>

                                                                ...
```

124

OVAL: esempio

```
...
<tests>
      <registry_test id="oval:org.mitre.oval:tst:4279" version="2" comment="SharePoint Server 2007 is installed."
        check_existence="at_least_one_exists" check="at least one">
            <object object_ref="oval:org.mitre.oval:obj:2686"/>
            <state state_ref="oval:org.mitre.oval:ste:3235"/>
      </registry_test>
      <file_test id="oval:org.mitre.oval:tst:9391" version="1" comment="the version of Mssdmn.exe is less than
        12.0.6031.5000" check_existence="at_least_one_exists" check="at least one">
            <object object_ref="oval:org.mitre.oval:obj:1840"/>
            <state state_ref="oval:org.mitre.oval:ste:4572"/>
      </file_test>
</tests>
...
```

125

OVAL: esempio

```
...
<objects>
      <registry_object id="oval:org.mitre.oval:obj:2686" version="1">
            <hive>HKEY_LOCAL_MACHINE</hive>
            <key>SOFTWARE\Microsoft\Office\12.0\Registration\{90120000-110D-0000-0000-0000000FF1CE}</key>
            <name>ProductName</name>
      </registry_object>
      <file_object id="oval:org.mitre.oval:obj:1840" version="1">
            <path var_ref="oval:org.mitre.oval:var:834" var_check="all"/>
            <filename>Mssdmn.exe</filename>
      </file_object>
      <registry_object id="oval:org.mitre.oval:obj:281" version="1" comment="The registry key that identifies the location
        of the common files directory.">
            <hive>HKEY_LOCAL_MACHINE</hive>
            <key>SOFTWARE\Microsoft\Windows\CurrentVersion</key>
            <name>CommonFilesDir</name>
      </registry_object>
</objects>
...
```

126

OVAL: esempio

```
...
<states>
      <registry_state id="oval:org.mitre.oval:ste:3235" version="2" comment="The registry key has a value of Microsoft
        Office SharePoint Server 2007">
            <value>Microsoft Office SharePoint Server 2007</value>
      </registry_state>
      <file_state id="oval:org.mitre.oval:ste:4572" version="1">
            <version datatype="version" operation="less than">12.0.6318.5000</version>
      </file_state>
</states>
<variables>
      <local_variable id="oval:org.mitre.oval:var:834" version="1" comment="The SharePoint BIN directory"
        datatype="string">
            <concat>
                  <object_component item_field="value" object_ref="oval:org.mitre.oval:obj:281"/>
                  <literal_component>\Microsoft Shared\web server extensions\12\BIN</literal_component>
            </concat>
      </local_variable>
</variables>
</oval_definitions>
```

127

Common Attack Pattern Enumeration and Classification (CAPEC)

- capec.mitre.org
- linguaggio per descrivere azioni e sequenze di attacco
- in via di sviluppo

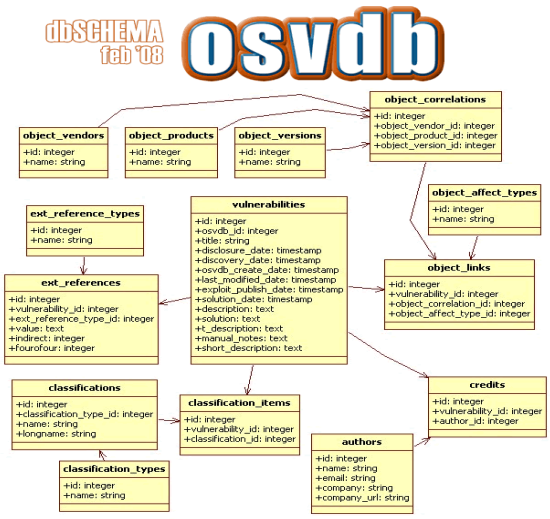
128

Open Source Vulnerability Database (OSVDB)

- **osvdb.org**
- **database di vulnerabilità independente e open source**
  - vulnerabilità
  - prodotti vulnerabili
  - riferimenti esterni
  - classificazioni
  - possibili soluzioni
- **consultabile online**
- **export in XML, CSV, MySQL/SQLite**

129

OSVDB



fonte: OSVDB.org

130

Modello strutturato delle vulnerabilità

- **utilizza la stessa rappresentazione del modello vulnerabilità**
  - espandendo il grafo con informazioni su:
    - presenza di vulnerabilità
    - presenza di errori di configurazione
    - eventuali informazioni su parametri rilevanti nella configurazione del sistema come visto per OVAL
    - eventuali informazioni sui pattern di attacco
  - e usando gli usali operatori logici per relazionarle con le possibili conseguenze

131

Riferimenti

- **ISO (www.iso.org)**
  - serie 27000, in particolare ISO 27001 e ISO 27005
- **MAGERIT**
  - www.csi.map.es/csi/pg5m20.htm
- **EBIOS**
  - www.ssi.gouv.fr/fr/confiance/ebiospresentation.html
- **OCTAVE**
  - www.cert.org/octave/

132

Riferimenti

- **NIST (csrc.nist.gov)**
  - serie SP 800, in particolare 800-30
  - NVD (nvd.nist.gov)
- **MITRE (www.mitre.org)**
  - enumerazioni, linguaggi: measurablesecurity.mitre.org
- **OWASP (owasp.org)**

133