AKSILIA® Group

Strategy & Technology

VA & PT come strumenti del processo di analisi e valutazione del rischio informatico.

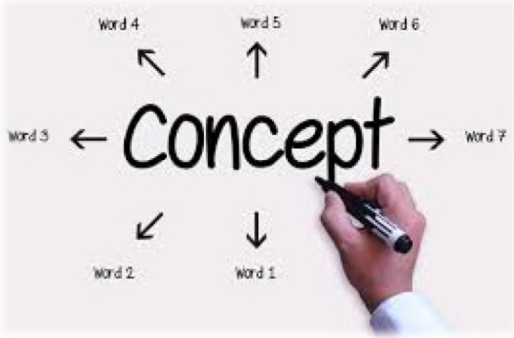
Matteo Mazzei

PISA 17/07/2020

Nato nel 1973 a Lucca, laureato a Pisa in **Ingegneria delle Telecomunicazioni** nel 2000. Oltre **20 anni** di esperienza in ambito ICT con **focus** su **networking** e **security**. Ha iniziato il suo percorso lavorativo in **CSELT**, il centro di ricerca e sviluppo del gruppo TIM come network engineer lavorando sui progetti che hanno guidato l'evoluzione della rete attraverso l'implementazione dell'MPLS ed il transito di tutto il traffico voce in VoIP.

Ha rivestito dal 2003 al 2009 il ruolo di **NOC e SOC Manager** in **Infogroup Spa**, direzione dei sistemi informativi della Cassa di Risparmio di Firenze (ora parte del gruppo Engineering) gestendo la sicurezza ed il networking della server farm, il contratto TIM di CRF e coordinando un gruppo di 5 collaboratori. Dal 2009 al 2015 ha lavorato in **Fastweb** come **Senior Presale Engineer** supportando la forza vendita nella attività di progettazione e offering contribuendo allo startup del canale medium in Toscana, Marche e Umbria raggiungendo oltre **2,5 M€** di fatturato annuo. Dal 2015 ricopre ruoli di **CTO** (2015-2018 **Hisolution Srl**), **Solution Manager** (2018-2019 **7Layers Srl**) e **CISO** (2019 **Aksilia Group**) specializzandosi nella progettazione e implementazione di modelli miranti a tutelare e gestire il patrimonio informativo aziendale.

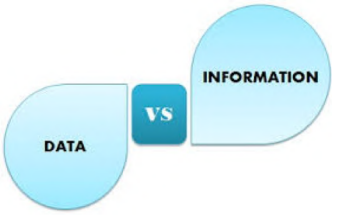
Iniziamo a inquadrare il problema delineando i contorni del contesto all'interno del quale si opera con alcune definizioni e concetti ....



In informatica, il termine "**dato**" indica un valore, tipicamente numerico in **bit**, che può essere elaborato e/o trasformato da un elaboratore elettronico utilizzando programmi sw che implementano algoritmi. Il dato rappresenta rappresenta una misura dal campo, in cybersecurity l'esempio di «dato» è rappresentato da un **LOG** raw o da elementi di **TELEMETRIA** raccolte da un agent su un end-point.

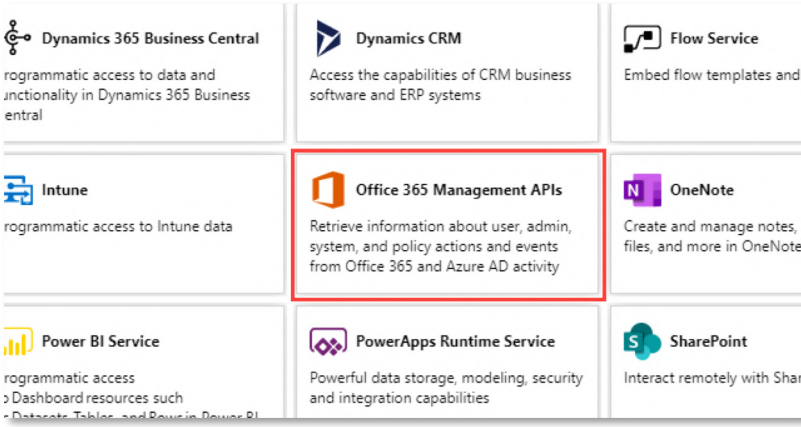
Informazione è il risultato di un'elaborazione di dati ed è data dall'insieme di più dati **correlati** tra loro, **organizzati**, **strutturati**, **analizzati** e arricchiti da **CONTESTO**. Un'informazione ha valore in quanto potenzialmente utile al fruitore per i suoi molteplici scopi.

La differenza principale tra dato e informazione è che l'informazione è «**AZIONABILE**» ovvero permette all'utilizzatore di prendere delle decisioni.



CONTESTO

- Siete un **SECURITY ANALYST** di un'azienda manifatturiera, il cui core business è produzione e vendita di scarpe. L'azienda per cui lavorate ha 500 dipendenti e un fatturato 100 M€.
- E' presente un **ufficio amministrazione** guidato dal CFO che è responsabile di 10 collaboratori.
- L'azienda ha acquistato i servizi **Microsoft365**. Su **Azure Active Directory** avete attivato sia l'**audit logging** che l' **activity auditing**.
- Fate uso di una piattaforma **email anti-malware** per proteggere gli utenti dalle minacce che utilizzano la posta come vettore di attacco.
- Avete in produzione un **SIEM** che raccoglie i **LOG** generati da Azure AD e dalla piattaforma di email antimalware.



Office 365 Management APIs box.

Oggi ricevete degli **alert** da Azure AD e dalla piattaforma email antimalware in particolare:

- L'alert generato da Azure AD vi informa che ci sono stati **200** tentativi di **login falliti** sugli account della vostra organizzazione.
- L'alert generato dalla piattaforma email antimalware vi informa che avete ricevuto **1000** email classificate come tentativi di **phishing** verso le caselle di posta della vostra organizzazione.

Questi sono dati o informazioni?

Presi singolarmente sono **dati** (non sono azionabili). Infatti da buon security analyst sapete che la vostra organizzazione subisce molti tentativi di **CREDENTIAL STUFFING**, attacchi di tipo **PASSWORD SPRAY** o **BRUTE FORCE** ogni giorno e che sempre giornalmente riceve molte email di **PHISHING**.

MA SE .....

..... Una regola che avete opportunamente configurato sul SIEM vi informa che dei 200 tentativi di Login falliti **150** sono relativi a un insieme di **10** account (**ELABORAZIONE, SINTESI E ORGANIZZAZIONE DEI DATI**) e che delle 1000 email di phishing ricevute **700** avevano come destinatarie solo **10** cassette di posta (**ELABORAZIONE, SINTESI E ORGANIZZAZIONE DEI DATI**) e soprattutto che i 10 account utente oggetto dei tentativi di Login falliti sono gli stessi a cui sono associati gli indirizzi email oggetto del phishing (**CORRELAZIONE** dei dati elaborati, organizzati e sintetizzati) ..... Iniziate a DRIZZARE LE ORECCHIE!

SE POI ..... andando a controllare a chi appartengono gli account scoprite che sono tutti i colleghi dell'ufficio acquisti (**+ CONTESTO**) allora avete un'informazione: l'ufficio acquisti della vostra azienda è il target di un attacco mirato (probabilmente un BEC) e potete prendere delle decisioni (**INFO. AZIONABILE**) . Avvertire gli utenti stringere le maglie, aumentare la sorveglianza, aumentare il livello di logging e alerting.

SICUREZZA INFORMAZIONI: è l'insieme delle attività volte a proteggere e tutelare il patrimonio informativo di un'organizzazione.

La sicurezza delle informazioni si misura su 3 dimensioni:

- Confidenziality
- Integrity
- Availability

I dati o le informazioni non devono aver subito modifiche **NON AUTORIZZATE**

I dati o le informazioni devono essere **DISPONIBILI** a chi è autorizzato e ne richiede l'accesso in un **TEMPO CONGRUO** con il compito che deve svolgere

I dati o le informazioni devono essere accessibili **SOLO** a chi è **AUTORIZZATO**

La sicurezza delle informazioni si fonda sui seguenti elementi:

- **Organizzazione** = ruoli/responsabilità + processi/procedure;
- **Persone**;
- **Strumenti** (a supporto dei processi e utilizzati dalle persone).

La **SICUREZZA DELLE INFORMAZIONI** ha come oggetto tutti gli asset informativi di un'azienda.

Un **ASSET INFORMATIVO** è qualunque elemento coinvolto nel ciclo di vita delle informazioni che abbia valore per l'organizzazione.

UN ESEMPIO

DENOMINAZIONE	AREA RESP.	TIPOLOGIA	CRITICITÀ	SERVIZI IMPATTATI	DESCRIZIONE
Processi/Attività - Asset primari	Vari	Information Asset	5	Tutti	I processi e le attività svolte con l'asset (ad esempio sviluppo software, supporto clienti, gestione fornitori, ecc.)
Informazioni - Asset primari	Vari	Information Asset	5	Tutti	Database o datafile, documentazione di sistema, manuale utente, materiale didattico, procedure operative, piano di continuità;
Hardware - Asset di supporto	IT	Asset fisici	3	Tutti	Computer, Server, supporti fisici, apparati (alimentatori, aria condizionata, ecc.), SAN, stampanti, UPS
Software - Asset di supporto	IT	Information Asset	3	Tutti	Software applicativo, software di sistema, tool di sviluppo, utility, VM;
Reti - Asset di supporto	IT	Asset fisici	3	Tutti	Firewall, router, switch, centri stella, apparati core network, ecc.
Personale - Asset di supporto	Vari	Risorse umane	4	Tutti	Dipendenti, collaboratori, consulenti
Sito - Asset di supporto	Vari	Asset fisici	3	Tutti	Locale / sede presso cui l'asset è utilizzato
Struttura organizzativa - Asset di supporto	Vari	Risorse umane	3	Tutti	La funzione organizzativa cui l'asset è stato assegnato (Area servizi, Area produzione, Area commerciale, Area assistenza/progetti)

CYBER SECURITY rappresenta un campo relativo alla sicurezza informatica che comprende strumenti e tecnologie la cui funzione è quella di proteggere i sistemi informatici dagli attacchi. E' tutto ciò che protegge l'azienda e gli individui da **attacchi intenzionali**, violazioni o incidenti, e dalle loro conseguenze. La cyber security è focalizzata principalmente sulla protezione dei sistemi informatici (computer, reti di telecomunicazione, smartphone, ecc.) e **dell'informazione in formato digitale** da attacchi interni e, **soprattutto, esterni**. Nella Cyber Security sono presenti elementi giuridici, umani, tecnici e organizzativi in grado di analizzare i punti vulnerabili di un sistema, le minacce e i rischi associati.

DIFFERENZE

ITEM	CYBERSECURITY	SICUREZZA DELLE INFORMAZIONI
TIPOLOGIA DI DATI/INFORMAZIONI	Solo digitali.	Tutte (es: archivi cartacei).
ASSET	Hw, Sw, Informazioni.	Processi, Persone, Siti/Sedi, Strutture Organizzative.
FOCUS	Principalmente sul tenere fuori i cattivi (riservatezza), integrità (e autenticità), poco sulla disponibilità (quasi solo per attacchi DoS/DDoS).	Riservatezza, Integrità, Disponibilità. Ad esempio i processi di backup, disaster recovery, business continuity non rientrano nello scope della cyber security mentre sono centrali nella sicurezza delle informazioni.
THREAT MODEL	I *threat actor* considerati sono solo «umani» e le minacce sono dovute a azioni «dolose» ed intenzionali.	Le minacce considerate comprendono eventi «accidentali» come epidemie, scioperi, blackout e ambientali/naturali come incendi, allagamenti, terremoti. Tra le minacce apportate da *threat actor* «umani» abbiamo anche gli errori (che non sono compresi nella cybersecurity)
BUSINESS	**Lontana** dal business (mitigazione di minacce e vulnerabilità tipicamente note, che prevedono risposte prevalentemente tecniche)	**Vicina** al business (sicurezza delle informazioni è competenza di una “security governance”, di un CSO e/o del CISO, collocati organizzativamente ad un livello tale da consentire un’interlocuzione adeguata con il business

Per quanto detto risulta ormai chiaro che .....

$\supseteq$

E' un sottoinsieme di...

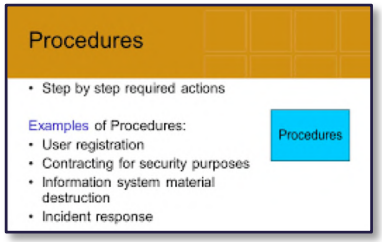
*.... e che le **informazioni** costano **€**! Costa crearle, costa acquistarle soprattutto costa **gestirle**!*

La **Sicurezza delle Informazioni** è governata dal **Sistema** di **Gestione** della **Sicurezza Informatica** (SGSI).

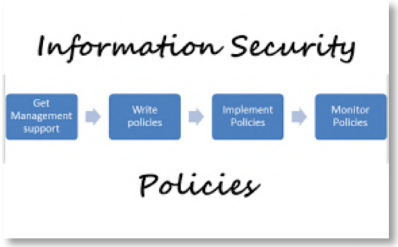
SGSI: è un *framework* composto da attività, risorse, strumenti, persone, ruoli, responsabilità, informazioni, processi e procedure, impiegate da un'organizzazione per **raggiungere** e **mantenere** gli **obiettivi** di sicurezza delle informazioni definiti in termini di *riservatezza, integrità e disponibilità.*

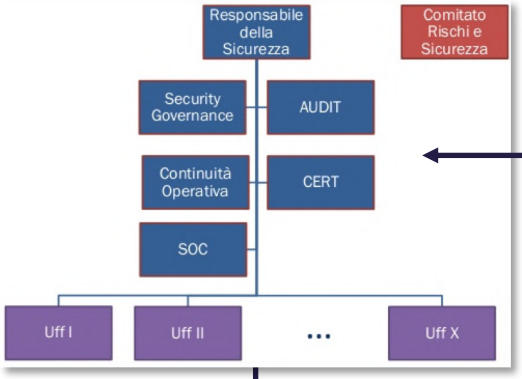
…. Più in dettaglio un **SGSI** permette di *controllare*, *monitorare* e *tutelare* il **patrimonio informativo** aziendale e si compone, quindi, di:

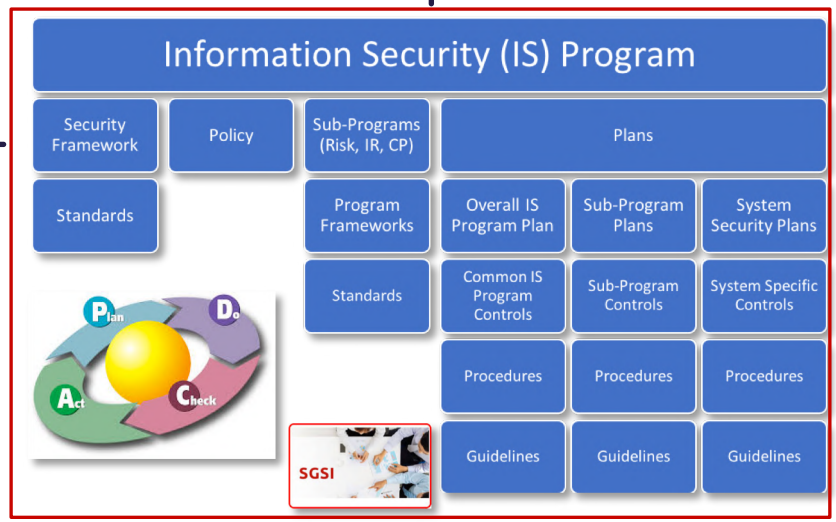
- ✓ un' organizzazione = ruoli + responsabilità;
- ✓ politiche di sicurezza;
- ✓ Processi e procedure operative (istruzioni);
- ✓ controlli fisici (relativi all'ambiente di lavoro ed alle attrezzature…);
- ✓ controlli logici (relativi ai servizi ICT…) ;
- ✓ Cultura.

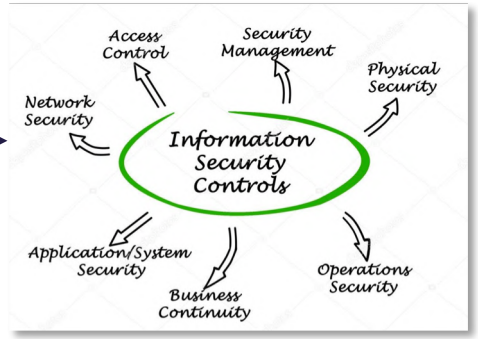

Procedures
• Step by step required actions
Examples of Procedures:
• User registration
• Contracting for security purposes
• Information system material destruction
• Incident response
Procedures

IDENTIFY RISK
SECURITY PROCESS
ASSESS
IMPLEMENT CONTROLS


Information Security
Get Management support
Write policies
Implement Policies
Monitor Policies
Policies


Responsabile della Sicurezza
Comitato Rischi e Sicurezza
Security Governance
AUDIT
Continuità Operativa
CERT
SOC
Uff I
Uff II
...
Uff X


Information Security (IS) Program
Security Framework
Policy
Sub-Programs (Risk, IR, CP)
Plans
Standards
Program Frameworks
Overall IS Program Plan
Sub-Program Plans
System Security Plans
Standards
Common IS Program Controls
Sub-Program Controls
System Specific Controls
Procedures
Procedures
Procedures
Guidelines
Guidelines
Guidelines
Plan
Do
Check
Act
SGSI

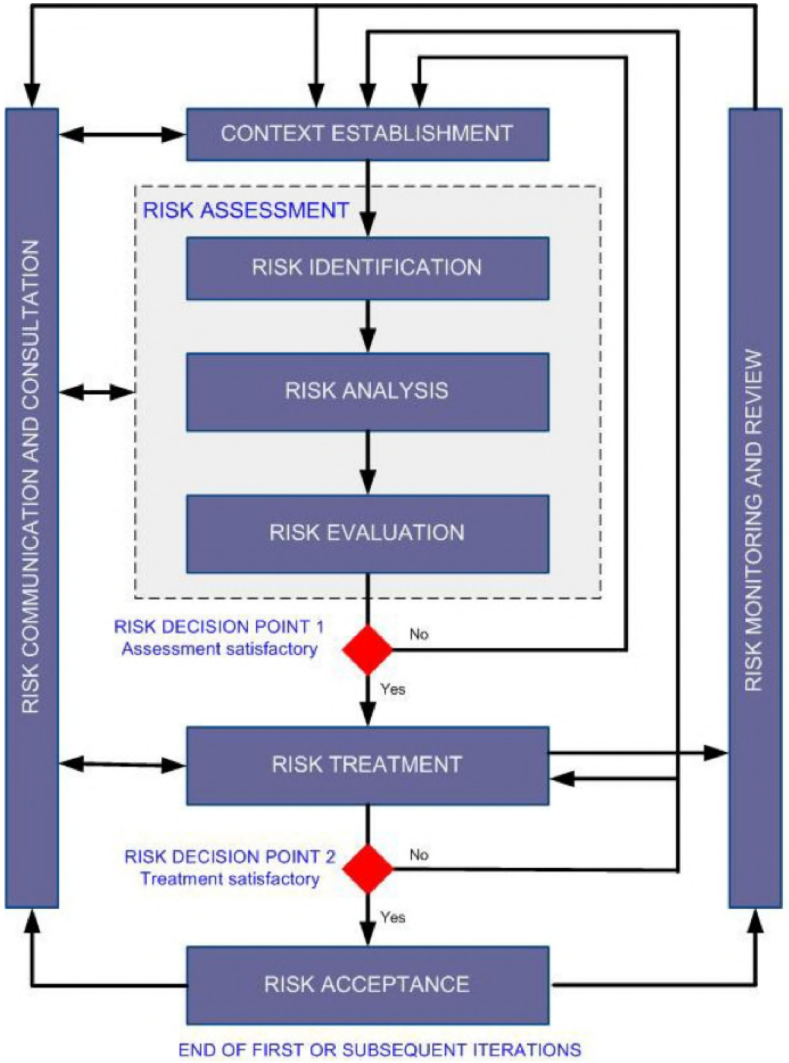

Access Control
Security Management
Physical Security
Network Security
Information Security Controls
Application/System Security
Business Continuity
Operations Security

Roles and Responsibilities!

ACCESS CONTROL
TRACKING
DATA
INTRUSION
INTERCOM
VIDEO
TURNSTILES
BIOMETRICS

Security Awereness and Policy Training

Il processo di **RISK MANAGEMENT** è il **motore** di ogni Sistema di Gestione della Sicurezza Informatica.



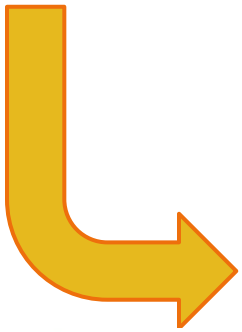
- **Bene**: qualunque cosa a cui l'azienda attribuisce un valore. Gli asset informativi (dati, informazioni, strumenti tecnologici, persone processi etc) hanno un valore.
- Il **valore** di un asset è costituito dalla sua «utilità» nel raggiungere gli obiettivi prefissati dall'azienda e si esprime nell'impatto a seguito di un incidente che ha come oggetto quell'asset.
- Gli **impatti** di un incidente possono **causare** delle **perdite**.
- Una **minaccia** è qualcosa che può condurre a un incidente che impattando su uno o più beni può causare delle **perdite**.
- Le minacce sfruttano le **vulnerabilità** presenti all'interno di un'organizzazione (sistemi, applicazioni e servizi) per danneggiare dei beni.
- **Rischio:** rappresenta la potenzialità che una minaccia sfrutti le vulnerabilità presenti nell'organizzazione per causare perdite e danni a uno o più beni. Il rischio si misura moltiplicando il valore assegnato al bene per il livello di criticità della vulnerabilità e la «verosimiglianza» che si verifichi la minaccia

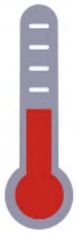
RISK ASSESSMENT: è un processo che ha lo scopo di ***identificare*** tutti i rischi a cui è soggetta un'organizzazione, di ***valutarli*** (assegnandogli un valore), di ***ponderarli*** (definendo il «**criterio di rischio**», ovvero quel valore al sotto del quale i rischi possono essere accettati dall'organizzazione, e confrontandoli con il «criterio di rischio» per ricavare i rischi da trattare).

(1) Identificazione degli asset, attribuzione del valore (impatto) a ogni asset, **(2)** identificazione delle minacce, **(3)** valutazione delle minacce (verosimiglianza), (4) identificazione delle vulnerabilità, **(5)** valutazione delle vulnerabilità.

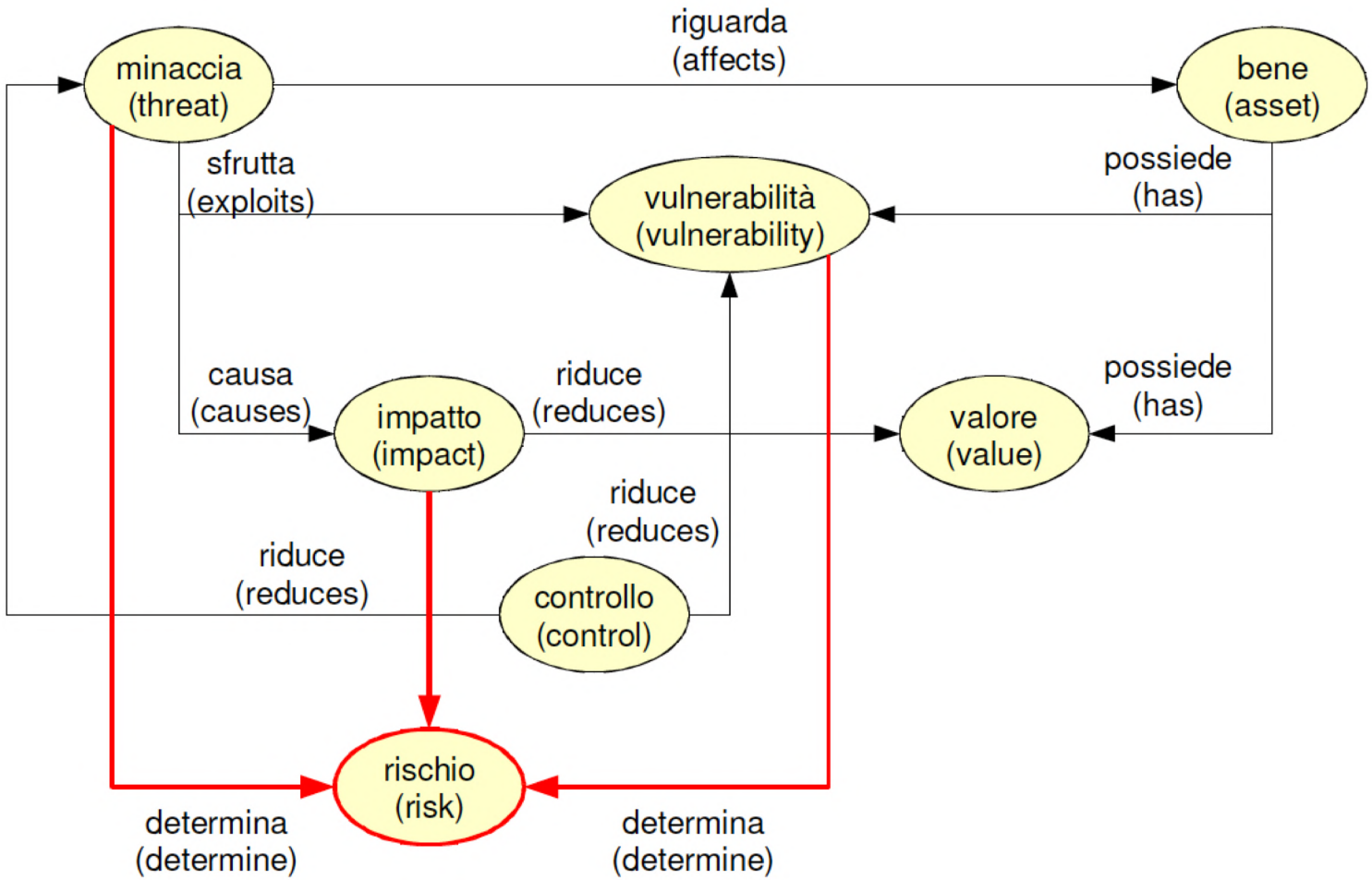
Per ogni asset viene calcolato il **rischio** moltiplicando: il **valore dell'asset * la verosimiglianza di ogni minaccia * il livello di vulnerabilità**. A parità di asset questo viene ripetuto per ogni vulnerabilità che può sfruttare la minaccia.

RISK MANAGEMENT: è un processo che ha lo scopo di trattare i rischi applicando contromisure e/o controlli per raggiungere un livello di rischio residuo compatibile con le esigenze di business dell'organizzazione (inferiore al livello di «**criterio di rischio**» stabilito).





Per ogni asset il cui rischio sia **superiore** al livello del «**criterio di rischio**», si identificano le modalità di trattamento: **eliminare/evitare il rischio** (es: rinuncio/interrompo/annullo l'attività/asset a cui è associato il rischio), **trasferire/condividere il rischio** (es. stipulo un'assicurazione, stipulo un contratto con un fornitore esterno completo di penali), **mitigare il rischio** (modificando la probabilità delle minacce alla base), **contenere il rischio** (modificarne le conseguenze in modo da ridurne l'impatto).


minaccia
(threat)
riguarda
(affects)
bene
(asset)
sfrutta
(exploits)
vulnerabilità
(vulnerability)
possiede
(has)
causa
(causes)
impatto
(impact)
riduce
(reduces)
valore
(value)
possiede
(has)
riduce
(reduces)
riduce
(reduces)
controllo
(control)
rischio
(risk)
determina
(determine)
determina
(determine)

- ***ESEMPIO DI ANALISI DEL RISCHIO***

- ***ESEMPIO DI PIANO DI TRATTAMENTO DEL RISCHIO***

Esempio: da ISO 27001-ISO 27005

Un **SECURITY AUDIT** è una valutazione sistematica della sicurezza del sistema informativo di un'azienda o di una sua parte, misurando la sua conformità a una serie di criteri stabiliti. E' un modo in cui un'organizzazione può testare e valutare la propria '**security posture**'. Gli audit di sicurezza vengono spesso utilizzati per determinare la conformità normativa , es: GDPR, oppure il rispetto di requisiti espressi da standard, es: ISO 27001. Gli audit si dividono in:

- AUDIT DI **PRIMA** PARTE: noti come audit interni. Questo è quando un membro dell'organizzazione stessa effettua l'audit. Questa persona può essere un dipendente dell'organizzazione o qualcuno assunto dall'organizzazione per eseguire gli audit interni, come un consulente, ma l'importante è che la persona agisca per conto dell'azienda piuttosto che un cliente o un ente di certificazione.

IT SECURITY AUDIT

- AUDIT DI **SECONDA** PARTE: Gli audit di seconda parte sono delle verifiche eseguite dai clienti nei confronti dei loro (potenziali o effettivi) fornitori. Per questa tipologia di audit le grandi aziende possono avvalersi, oltre che del proprio personale, di società di consulenza specializzate proprio in questo business.

- AUDIT DI **TERZA** PARTE: il cui scopo è il rilascio di un certificato, è condotto da un ente esterno, tipicamente incaricato da un organismo di certificazione, autorizzato dotato delle opportune caratteristiche di affidabilità e imparzialità.

IL VA E IL PT SONO AUDIT *(TIPICAMENTE DI PRIMA O SECONDA PARTE)*

VULNERABILITY ASSESSMENT

E' un'attività di **identificazione** e **analisi** delle **vulnerabilità** presenti in un ambiente. Costituisce una **fotografia** dello stato dell'ambiente analizzato in un preciso istante.

Le vulnerabilità rilevate **non sono sfruttate**.

Consente ad una azienda di **riconoscere** e **scoprire** le **debolezze** della propria infrastruttura ICT.

PENETRATION TEST

E' un processo **più ampio** che **comprende** anche un vulnerability assessment.

Il *pentest* **valida** la vulnerabilità trovata attraverso lo sfruttamento della stessa.

NOTA: *un pentest comporta il* ***rischio*** *di* ***cambiare*** *o* ***danneggiare*** *l'ambiente target!*

NOTA: sono tipologie di analisi ***dinamica*** dei sistemi. Valutano sw e fw «***running***» oltre che a configurazioni e variabili di ambiente.

VULNERABILITY ASSESSMENT

Il destinatario di questa attività è l'azienda che ha bisogno di **fotografare** lo stato della propria infrastruttura per **comprendere e valutare il rischio ICT** o per esigenze di compliance (ISO, NIST, GDPR).

Per esigenze operative e di *business continuity*, i sistemi target non possono essere compromessi o la loro operatività ridotta.

PENETRATION TEST

Viene richiesto quando un'azienda ha una conoscenza abbastanza chiara dei propri punti deboli e ha bisogno di **verificare** la reale possibilità di **sfruttamento** delle vulnerabilità.

I sistemi analizzati possono essere compromessi.

Anche il PT è spesso richiesto per esigenze di compliance a normative operative cogenti.

Gli **STAKEHOLDER** delle attività di Vulnerability Assessment e Penetration Test coinvolte e/o interessate sono:

- **EXECUTIVE/TOP MANAGEMENT**: per raggiungere il successo desiderato nel programma IT security, il top management deve **supportare** l'attività **allocando** tutte le risorse necessarie. A questi interlocutori interessano informazioni di «**alto**» livello, indicatori **semplici** da comprendere e informazioni **facilmente** assimilabili. A queste persone bisogna parlare con **numeri collegando** i rischi a possibili **perdite** economiche e **conseguenze** per il business. Il tipo di report adatto a questi interlocutori è la **scorecard**.

- **HEAD OF IT SECURITY:** di solito questa posizione riporta direttamente al executive/top management, fornendo una visione dall'alto della «**security posture**» dell'infrastruttura ICT dell'organizzazione al top management. E' una persona competente in grado di comprendere informazioni tecniche. E' interessato a capire «**se**» la situazione sia negativa e «**quanto**» lo sia, e a avere una stima **dell'effort** necessario a risolvere i problemi. Il tipo di report adatto a questo interlocutore è un report delle attività **prioritizzate** in base al **rischio** (l'impatto sui sistemi e la probabilità che si possa concretizzare la minaccia) che consenta di **impostare**, **gestire** e **coordinare** le attività di remediation.

- **SecOps**: Sono figure con **spiccate** competenze tecniche, sono interessati agli **interventi** di remediation da effetttaure. I report adatti a questi interlocutori devono **evidenziare** le vuln più critiche (0-day, quelle che interessano i sistemi business critical, le vulnerabilità «facilmente» sfruttabili, quelle sulle quali sono già stati osservati attacchi «*in the wild*», quelle per le quali sono disponibili sul web exploiting script e tools di exploiting). Si aspettano un remediation report dove gli interventi saranno prioritizzati in base ai criteri sopra esposti:

- **Ops/SysAdmin**: sono i gruppi che **applicheranno** le patch. Queste figure sono interessate a sapere **quali** sistemi patchare/fixare e in che **ordine** di priorità. Si aspettano un «**patch report**» che elenchi i sistemi da patchare e l'ordine in cui patcharli.

BLACK BOX

Utilizzata per **simulare** un attaccante **privo** di informazioni specifiche, tipicamente esterno, con questo modello sono noti solamente i seguenti elementi:

- Scope dell'attività
- Timing dell'attività
- Regole di ingaggio

WHITE BOX

La **visibilità** del target è **completa**: con questo modello sono noti, oltre ai dati del modello black box, anche:

- Struttura interna
- Design
- Implementazione dei sistemi

es. configurazione firewall, codice sorgente, funzioni delle subnet, ruoli e profili di accesso, etc.

GRAY (O GREY) BOX

Utilizzata per simulare un attaccante interno, con questo modello sono note informazioni parziali sul sistema target.

Ad esempio è nota la struttura interna ma non il codice degli applicativi testati.

FLUSSO ATTIVITÀ

1. **Pre-Engagement Interactions:** definire le regole di ingaggio, target, orari,
2. aspetti legali
3. **Identificazione** del perimetro (tutti gli asset in scope)
4. **Configurare la piattaforma** di SCAN
   a. Inserire i target (IP, FQDN, IP RANGES, URL).
   b. Configurare le modalità dello SCAN (banda utilizzata, porte testate, eventuaIe record di autenticazione per sistemi e form di autenticazione per applicazioni)
5. **Lanciare o schedulare lo SCAN** (se deve essere effettuato in un orario particolare)
6. **Interpretare** i risultati
7. **Individuare** gli stakeholder destinatari di un report
8. **Creare un report custom** per massimizzarne la fruibilità del destinatario (Scorecard Report per Executives, Remediation Report per gli Infosec, Patch Report per le Ops.)
9. **Presentazione** del Report

FLUSSO ATTIVITÀ

1. **Pre-Engagement Interactions:** definire le regole di ingaggio, i target, gli obiettivi, gli orari e/o date, gli aspetti legali
2. **Reconnaissance or Open Source Intelligence (OSINT) Gathering:** riccerca e raccolta delle informazioni che potrebbero essere utili nelle fasi successive. Google Dorks, Social Engineering, Whois, Shodan, Censys
3. **Discovery and Scanning:** le informazioni raccolte vengono utilizzate per eseguire attività di rilevamento per determinare elementi come porte e servizi disponibili per host o sottodomini e per applicazioni Web.
4. **Vulnerability Assessment**
5. **Exploitation:** dopo aver interpretato i risultati del VA, i pen tester useranno tecniche manuali, intuizione e il loro background tecnico per convalidare, attaccare e sfruttare tali vulnerabilità.
6. **Final Analysis and Review:** descrizione di dove è iniziato il test, come sono state rilevate le vulnerabilità e come sono state sfruttate. Include anche l'ambito dei test di sicurezza, le metodologie di test, risultati e raccomandazioni per le correzioni.

Metodologie implementate:

- OWASP (Open Web Application Security Project)

https://www.owasp.org/index.php/Main_Page

- OSSTMM (Open Source Security Testing Methodology Manual)

http://www.isecom.org/research/

- PTES

http://www.pentest-standard.org/index.php/Main_Page

Criteri di Classificazione

- CVSS2/3 (Common Vulnerability Scoring System Version 2/3.0

https://www.first.org/cvss/calculator/3.0

https://www.first.org/cvss/calculator/2.0

A livello formale sono richiesti i seguenti documenti:

- Regole di ingaggio

- NDA

E soprattutto ....

..... **MAI** dimenticare la

- Manleva!

COMMERCIALI €€

RAPID7

Nessus vulnerability scanner

Qualys

IBM QRadar

SKYBOX SECURITY

acunetix

MALTEGO

BURPSUITE

FREE €€

BURPSUITE COMMUNITY EDITION

OpenVAS Open Vulnerability Assessment Scanner

NMAP

Tools e script presenti nelle distro customizzate come:

KALI

metasploit

w3af

WPScan

Nikto

Siete il **CISO** di un'azienda manifatturiera che si occupa di produzione e vendita di scarpe. L'azienda ha un fatturato **100 Mil€** di cui **50 Mil€** dalla vendita tramite **negozi** e **50 Mil€** tramite una piattaforma di **e-commerce**. L'azienda ha una unica sede, e circa **500** dipendenti.

L'infrastruttura ICT dell'azienda è composta da :

- Una rete Lan interna su cui sono attestati sia gli end point utente che i server;
- Una rete Lan di produzione su cui sono attesati i PLC delle linee di produzione gli apparati DCS, HMI, stampanti industriali wifi, pistole a barre wifi;
- L' e-commerce è gestito dal personale interno, sviluppato da un fornitore terzo e si trova su un hosting provider esterno.
- Due reti wifi, una che corrisponde alla Lan interna (condivisa tra utenti interni e guest) una che corrisponde alla Lan produzione sono collegati pistole, stampanti, tablet rugged

Tutte le reti sono gestite da uno stack di switch L3 con un solo un Fw sul perimetro.

In particolare sulla rete ICS abbiamo:

- AP ormai obsoleti;
- stampanti industriali equipaggiate con micro-kernel android non aggiornati;
- I server e le stazioni Windows, ormai fuori supporto (WXP, W7, W2003/8 server), non sono aggiornate da tempo e non riceveranno più aggiornamenti, inoltre questi sistemi non sono più supportati neanche dai più comuni sistemi commerciali EPP/EDR;

La reti interne e dalla soprattutto dalla rete wi-fi sono raggiungibili senza nessun filtro tutti i sistemi attestai sulla rete di produzione. Il portale ecommerce in hosting, fa uso di Worpress (con plugin woocommerce) e di personalizzazioni in php, utilizza versioni di wordpress e php ormai obsolete.

.....Commissionate subito un VA/PT a un'azienda esterna per capire che altro troverete!

Il VA evidenzia che:

- tutti i sistemi in scope siano soggetti a un numero elevato di vulnerabilità con uno score **CVSS > 7,5** alcune delle quali risultano molto facili da sfruttare per un attaccante con abilità medio basse
- che sono già stati osservati attacchi *in the wild* che sfruttano le vulnerabilità rilevate e che tali attacchi utilizzano script/tools facilmente reperibil sul web

I sistemi ICS **non sono** facilmente **aggiornabili**, l'aggiornamento richiede l'intervento di tutti i fornitori del sistema SCADA, ha **tempi lunghi** e soprattutto costi molto **elevati** (dell'ordine di diverse centinaia di migliaia di €).

Anche il portale e-commerce **non può essere aggiornato** facilmente perché l'aggiornamento della versioni di wordpress e Php richiedono degli ulteriori sviluppi fatti per supportare le personalizzazioni. Anche in questo caso l'attività non è immediata.

..... ***COSA** FARE?*

1. **Segmentare** le reti inserendo un Fw di secondo livello (vendor differente da quello in uso) e **segregando** ambienti a cui corrispondono **profili di rischio differenti**. L'architettura della rete sarà modificata separando e segregando le subnet seguenti
   - uffici,
   - server interni (CRM, share, server AS, gestionale etc),
   - Lan produzione (ICS, HMI, MES,)
2. **Sostituire** gli AP con AP di nuova generazione gestiti direttamente dal nuovo Fw (che fungerà da controller) che vedrà le reti wi-fi pubblicate come interfacce gestendo l'accesso al livello wireless dei client e effettuando l'analisi del traffico attraverso motori IDPS (in grado di rilevare di rougue AP).
3. **Cambiare** la password della rete wifi di produzione e configurare AP in modo che SSID sia «**nascosta**»
4. Creare rete wifi guest con accesso mediante **captive portal** e credenziali *one-time* **a tempo**.
5. Configurare AP per permettere l'accesso alla rete wifi uffici mediante le **credenziali del dominio AD.**
6. Acquistare un WAF da anteporre al portale e-commerce in grado di ricevere in input l'output della scansioni del vulnerability scanner e fare **virtual patching** delle vulnerabilità rilevate.

Costo dell'investimento **200 K€**!

Di cui 150 K€ per il cluster di NGFW e gli AP e 50 K€ per il WAF.

..... A questo punto prendete l'analisi, chiedete **appuntamento** all'**AD** e gli dite «*ho commissionato un VA, **questo** è il report dell'attività che ha rilevato su tutti i nostri sistemi un gran numero di vulnerabilità con un CVSS (sia v2 che v3) **> 7,5**. Non possiamo patchare l'e-commerce aggiornando wordpress e php perché richiederebbe degli sviluppi e non possiamo aggiornare i sistemi della rete ICS/SCADA perché le patch non sono disponibili perché, **come lei saprà benissimo**, gli OS Windows XP, Vista, 2003 Server e 2008 Server sono andati fuori supporto. Per risolvere questi problemi mi servono **200.000 €** per acquistare un cluster di NGFW e dei nuovi access point con cui segmentare le reti e un WAF da mettere davanti al servizio e-commerce.*»

L'AD che **non è** un tecnico, il cui lavoro consiste nel trattare con i fornitori, nel trovare nuovi clienti, nel gestire gli aspetti finanziari e nel supervisionare le attività amministrative e che **vede valore** solo nei soldi spesi nel core business, ovvero in un nuovo magazzino o in una nuova macchina per una linea di produzione aggiuntiva cosa è più facile che vi risponda?

Risposta 1: grazie dell'analisi mi è tutto chiaro do subito indicazioni all'ufficio acquisti affinché si metta a disposizione per l'acquisto dei beni da lei indicati.

Risposta 2: non ho capito bene perché dovrei accordarle 200.000 € .... Come questa spesa può aiutare il nostro business di produzione e vendita di calzature?

Ma se ..... ricordandoci dell'analisi rischi diciamo all'AD.....

.... 3 anni fa abbiamo subito un attacco di phishing che utilizzando l'email come vettore aveva un *crypto-ranmsware* in allegato. A causa della scarsa formazione dei dipendenti l'allegato è stato aperto da un collega dell'uff. Acquisti e non essendoci alcun filtro nè segregazione tra le reti si è diffuso prima sui server, bloccando gestionale e CRM, e poi sulla rete di produzione bloccando le linee con il risultato che l'azienda è stata **ferma** per **3 gg**.....

COSTI INCIDENTE SICUREZZA €€:

- Valore della produzione di 3 gg: 100.000.000 M€/365*3 circa **822 K€**
- Penali dovute ai ritardi: 5% del valore della produzione giornaliero per ogni giorno, costo 3 gg circa **41 K€**
- Costi stipendi (ral media 35 K€): 134 € *500*3 circa **201 K€**
- Costi Fornitori chiamati a risolvere i problemi **20 K€**

COSTI TOTALI: 1,08 M€

PROBABILITA' INCIDENTE SICUREZZA €€: 1 volta ogni 3 anni circa il **33% di probabilità**

A questo punto è facile calcolare il **RISCHIO** di un incidente di sicurezza:

- **(P) PROBABILITA': 33%**
- **(I) IMPATTO: 1,08 M€**

(R) RISCHIO = P x I = **358 K€**

Le contromisure da voi adottate abbassano la probabilità di un incidente dal 33% al **5%**.

RISCHIO RESIDUO: P x I = **54 K€**

Dato che il costo **dell'investimento sull'infrastruttura** (**150 K€**) + il **rischio residuo** (**54 K€**) = **204 K€** è una somma **inferiore** del rischio corrispondente alla situazione attuale **358 K€**, l'investimento ha un ritorno economico di 358 K€-204 K€ = **154 K€**.

Ragionando in maniera simile per l'e-commerce faremo presente all'AD che un **Data Breach** sulla piattaforma di e-commerce può portare a una sanzione da parte del Garante della Privacy che può arrivare anche a un massimo tra 20 M€ di fatturato o il 4% del fatturato globale. Tuttavia alcuni studi (https://www.cybersecurity360.it/legal/privacy-dati-personali/sanzioni-gdpr-criteri-e-metodologia-di-calcolo-per-violazioni-alla-normativa-privacy/) hanno rilevato in Italia una sanzione media per violazioni di «gravità» media, come ad eesempio il mancato rispetto dei requisiti di sicurezza dei dati personali, pari a **310 K€**.

Oggi il numero delle imprese in Italia si aggira circa sui **4,4 Milioni** (https://www.istat.it/it/files/2019/12/C14.pdf) mentre il numero dei data breach tra il maggio 2018 e settembre 2019 (16 mesi) sono stati circa **1.500**. Da questo risulta che la probabilità che un'azienda in Italia subisca un Data Breach in una finestra temporale di 12 mesi è pari a = 1.500/4,4 Mil/16*12 che da un risultato di **0,025%**.

Dobbiamo però considerare che la **brand reputation** è strettamente connessa alla capacità di un'azienda di garantire un'adeguata protezione dei dati personali, e che pertanto a seguito di un data breach si ha:

- **DANNO EMERGENTE:** spese necessarie per ripristinare la propria reputazione (campagne online e offline ad hoc) valutate in un **3 %** del fatturato pari a **3 M€**.
- **LUCRO CESSANTE:** perdita dei clienti già acquisiti che decidono di recedere e/o risolvere i contratti a causa di tale danno, le statistiche (Ponemon Institute) parlano di un calo del **6,1%** di clienti a seguito di un Data Breach che equivale a una perdita di **6,1 M€**.
- **PERDITA CHANCE:** i potenziali clienti, saranno allontanati dalla vulnerabilità, e quindi inaffidabilità, dell'azienda stessa. Le statistiche (Ponemon Institute) parlano di un **35%** di riduzione del tasso di acquisizione di nuovi clienti. Supponendo un tasso di crescita del **10%** anno su anno il 35% di riduzione equivale a **3,5 M€** di perdite

A queste si devono aggiungere le sanzioni:

- **CIVILI:** risarcimento del danno e responsabilità solidale (difficilmente stimabili);
- **AMMINISTRATIVE:** prima valutate in **310 K€** circa;
- **PENALI:** reclusione da 6 a 36 mesi a seconda del reato commesso.

Facendo 2 conti abbiamo:

- **(P) PROBABILITA' DI DATA BREACH** = **0,025%**
- **(I) IMPATTO** = (0,31 M€+ 3,5 M€ + 6,1 M€ + 3 M€) = **12,91 M€**

(R) RISCHIO = P x I = **3.230 €**

Anche supponendo che il WAF azzeri la probabilità di Data Breach, azzerando di conseguenza anche il rischio residuo, dato che il costo **dell'investimento del WAF** **50 K€** è una somma **SUPERIORE** al rischio relativo alla situazione attuale **3,23 K€**, l'investimento avrebbe una perdita di 3,23 K€- 50 K€ = **- 46,77 K€**.

A seguito delle valutazioni effettuate:

L'investimento sull'infrastruttura interna sarà **approvato**;

L'investimento relativo all'acquisto del WAF sarà **bloccato**.

- I **VA** SI FANNO TOOLS AUTOMATICI

- LE PIATTAFORME DI **SCANNING** SONO IN GRADO DI:

  - ✓ confermare la presenza della vuln.
  - ✓ confermare se sono già stati effettuati attacchi a quella vuln. in the wild
  - ✓ Indicare il livello di competenza richiesto a un attaccante per sfruttare quella vuln.
  - ✓ Indicare se sono disponibili e facilmente reperibili tools per sfruttare quella vuln.

- I **PT** SI FANNO PER LO PIU' A MANO

- I **PT** RICHIEDONO MAGGIORI COMETENZE

- I **PT** RICHIEDONO PIU' TEMPO

- PERTANTO **PT** SONO PIU' COSTOSI

- I **PT** COMPRENDONO I VA DI CUI VALIDANO LE VULN. RILEVATE ATTRAVERSO LO SFRUTTAMENTO

In sintesi un **PT** **conferma** con certezza quello che una buona attività di VA già mi ha detto, ovvero che:

- ✓ La vuln. è presente
- ✓ Che è sfruttabile
- ✓ Che sono già disponibili dei tools/script che permettono di sfruttare la vuln.
- ✓ La difficoltà di exploiting, e quindi l'abilità richiesta a un attaccante per poter sfruttare la specifica vulnerabilità.

Se a questo aggiungiamo che:

- Il PT richiedendo più tempo e maggiori competenze di un VA è più costoso di un VA e quindi **raramente** lo si fa su **tutte** le vuln. rilevate
- Che **l'esito** del PT essendo un'attività per lo più eseguita manualmente **cambia** a seconda di chi lo fa e di che strumenti usa

…… **CI CHIEDIAMO**: « *Vale sempre la pena fare anche un PT di seguito al VA*?»

Valutando bene di cosa si ha bisogno spesso è **sufficiente** un **VA** ben fatto ed è possibile **evitare** il **PT**!

ATTENZIONE! Ci sono però situazioni in cui è consigliabile o addirittura mandatario fare un PT,… ad esempio:

- Quando è **impossibile applicare una patch o aggiornare i sistemi**, in questo avere la certezza che la vulnerabilità è sfruttabile e cosa il sistema compromesso permetterebbe di fare all'attaccante dà una misura cristallina del rischio.
- Quando il VA anche se ripetuto **non rileva** vulnerabilità o ne rileva troppo poche, indice di una situazione sospetta (*…davvero saremo stati così bravi …?*) vale la pena di effettuare un approfondimento.
- Quando è **esplicitamente richiesto** (audit di seconda parte) da parte di un cliente o in generale da uno stakeholder.

CI **CHIEDIAMO** ANCHE .....

*..... «dato che l'infrastruttura ICT di un'organizzazione è «**viva**» e cambia con il trascorrere del tempo seguendo i cambiamenti dell'organizzazione, ha senso fare un **VA** e **PT in** modalità **ONE-SHOT**?»*

.....E QUINDI..... «***COSA** FACCIAMO?*»

..... Considerando che .....un **VA** e/o **PT** *one-shot* sono meglio di ***niente*** ..... ciò che massimizza il **ROI** di un investimento in questa tipologia di attività è implementare un processo di **VULNERABILITY MANAGEMENT!**

Il **Vulnerability Management** è un **processo** per la gestione di vulnerabilità infrastrutturali, di sistema e applicative. Il VA/PT può esserne considerato eventualmente solo una **fase**.

È un **processo** mirato al **rilevamento** e alla **gestione** del **rischio** derivante dalla presenza di **vulnerabilità.**

Permette di

- costruire e mantenere aggiornato un **inventario degli asset** (*....quello che non si sa di avere non può essere gestito!*);
- di individuare le **vulnerabilità** e stimare i **rischi** della propria infrastruttura ICT;
- di identificare le remediation da implementare per fixare le vulnerabilità rilevate;
- fornisce un **input** «*efficace*» al processo di **patch management**;
- permette di controllare **l'efficienza** e **l'efficacia** dei gruppi incaricati delle remediation (patch e fix non applicate, storico delle vulnerabilità, efficacia delle remediation implementate)
- permette di valutare la **postura di sicurezza** degli ambienti analizzati

ASSET INVENTORY

Un elenco di tutti gli asset da cui selezionare quelli in scope per l'attività

INPUT

PIANIFICAZIONE

- Inserire gli asset selezionati nella piattaforma
- Configurare le modalità di scansione
- Identificare gli stakeholder dell'attività e l'output più opportuno per ognuno di loro

SCANNING

Raccolta e archiviazione di *audit evidence*

ANALYSIS

Analizzare gli output raw della piattaforma per
- verificare che l'attività si sia conclusa senza errori e/o anomalie
- Rilevare i sistemi che presentano più criticità e stabilire la modalità di reporting più idonea da produrre

REPORTING

PATCH REPORT

REMEDIATION REPORT

SCORECARD REPORT

REMEDIATION

Pianificazione ed esecuzione delle attività di remediation
- *Patching*
- *Hardening*

CONTROLLO

- Monitorare l'andamento dei lavori
- Verificare che le problematihe siano state risolte

RESCAN

PROCESSO VULN MNGT

Domande?

Grazie per l'attenzione!