Piano di gestione del rischio informatico: utility di supporto

Alessandro Brunengo

~~GDPR~~ ~~PDGR~~ PGR: cos'e'

- Il piano di gestone del rischio e' un documento che
  - descrive la procedura operativa per l'identificazione dei rischi informatici
  - definisce i criteri per gestirli (annullarli, mitigarli, accettarli)

- Le misure minime AGID impongono la definizione di un PGR che:
  - identifichi i rischi informatici
  - assegni ad ogni rischio un valore in funzione di:
    - importanza dei valori a rischio
    - tipologia del sistema vulnerabile
    - pericolosita' della minaccia
  - definisca il criterio di gestione di tali rischi, da applicare in ordine decrescente di valore del rischio

PGR: la sua funzione

Il PGR ha principalmente due scopi:

- definire di una procedura per
  - identificare i rischi
  - definire cosa fare: risolvere o mitigare, ove possibile e conveniente, accettare consapevolmente gli altri
- conseguentemente, acquisire consapevolezza di:
  - quali siano i valori del proprio Ente e dove siano collocati
  - quali siano le minacce che mettono a rischio questi valori

PGR dal punto di vista operativo

- identificazione dei valori dell'ente sulla propria rete locale, identificati e valutati in base ai criteri definiti nel PGR
- assegnazione di un "valore" a ciascun sistema presente sulla propria rete locale, in funzione dei valori esposti a pericolo in funzione di una ipotetica violazione di quel sistema
- identificazione delle minacce informatiche a cui ciascun sistema della rete e' vulnerabile
- assegnazione di un valore assoluto di pericolosita' a tali vulnerabilita' (come definito nel PGR)
- per ciascuno di questi rischi, definiti dalla combinazione di sistema-minaccia, assegnare un valore del rischio come definito dal PGR
- stilare un elenco ordinato dei rischi
- definire cosa fare per ciasun rischio, in ordine decrescente di valore, nei limiti definiti dal PGR

Utility a supporto: PGRlist

- Questa utlity ha lo scopo di
  - realizzare l'elenco dei sistemi presenti sulla rete locale
  - assegnare a ciascuno di questi un valore in R, I e D in funzione dei dati a cui tali sistemi hanno accesso

- l'implementazione attuale e' fatta tramite documento Excel
  - macro per l'automatizzare dei calcoli
  - mantenimento di uno storico degli elenchi su fogli dedicati
  - banale export in formato CSV (vedi altra utility)

  - Demo: https://proxy01.ge.infn.it/PGRlist.xls

PGRlist.xls: uso

- PGRlist.xls e' un documento excel in tre fogli, con i quali e' possibile
  - elencare le categorie di dati, assegnando i relativi valori in R, I e D
  - elencare le tipologie di sistema, associando a ciascuna di queste le categorie di dati a cui hanno accesso: una macro calcolera' il valore in R, I e D delle tipologie di sistema
  - elencare i sistemi presenti sulla rete locale, identificati via FQDN (supporto di wildcard) o IP (supporto di subnet), associando ciascuno di questi alle tipologie di sistema: una macro calcolera' automaticamente il valore in R, I e D di ciascun sistema

PGRlist.xls: uso (cont.)

- PGRlist dispone di una macro attivabile tramite pulsante per generare l'eleco dei sistemi con i loro valori su un foglio dedicato
  - e' possibile manenere uno storico delle configurazioni
  - e' possibile esportare tali dati su file CSV per l'utilizzo di PGReval

Utility a supporto: PGReval

- Questa utility ha lo scopo di combinare l'elenco dei sistemi e l'output di una scansione OpenVAS, per produrre l'elenco del rischi, ordinato in funzione del valore

- l'implementazione attuale e' una applicazione web, tramite la quale e' possibile fare upload di due documenti CSV e scaricare il risultato del calcolo in diversi formati
  - l'input file dell'elenco dei sistemi deve avere un formato analogo all'export CSV dell'elenco dei sistemi come realizzato tramite PGRlist
  - l'input della scansione OpenVAS e' un file CSV con il risultato della scansione esportato secondo il formato "results"

PGReval

- La web application PGReval
  - mantiene aggiornato un database con le vulnerabilita' informatiche pubblicate dall'NVE
  - accetta in upload l'elenco dei sistemi e l'output della scansione OpenVAS in formato CSV
  - Integra le informazioni sul valore delle vulnerabilita' con quelle pubblicate dal NIST sul National Vulnerability Database
  - produce in output l'elenco dei rischi, ordinato come previsto dal PGR
  - produce un log con un feedback sull'elenco dei sistemi
- Demo: https://proxy01.ge.infn.it

Sviluppi

- PGRlist
  - migliore controllo dell'input e gestione degli errori
  - evoluzione in una applicazione web based
    - backend su database
    - controllo di accesso
    - disponibilita' di storico

Sviluppi

- PGReval
  - aggiunta, automatica o a richiesta, di vulnerabilita' all'elenco generato da OpenVAS (possibili nuove vulnerabilita' ancora ignote ad OpenVAS)
  - backend su db, storico consultabile
  - supporto per un ricalcolo specifico del CVE di una vulnerabilita'
    - discriminare scansioni interne e esterne
    - inserimento di metriche temporali o di ambiente

Considerazioni sul PGR proposto

- Il PGR proposto e' una stesura ragionata, corretta e rivista
  - ma pur sempre la prima che sia stata fatta
- Non e' scolpita nella pietra: potra' subire revisioni
  - migliorare la praticabilita' operativa
  - coprire eventuali carenze
  - cambiare i criteri di valutazione dei valori e di identificazione delle vulnerabilita'
- E' probabile che la sua applicazione possa fornire indicazioni efficaci