Premio FORUM PA 2017: 10x10 = cento progetti per cambiare la PA

Documentazione di progetto della soluzione:

Regione Toscana Sicurezza Infrastrutturale, Perimetrale, ma non solo

INDICE

1. Descrizione progetto

2. Descrizione del team e delle proprie risorse e competenze

3. Descrizione dei bisogni che si intende soddisfare

4. Descrizione dei destinatari della misura

5. Descrizione della tecnologia adottata

6. Indicazione dei valori economici in gioco (costi, risparmi ipotizzati, investimenti necessari

7. Tempi di progetto

1. Descrizione progetto;

   Attivazione di misure di sicurezza per infrastrutture e servizi della seguente tipologia:

   - perimetrali
   - infrastrutturali
   - sistemi informativi
   - servizi iaas/paas/saas

2. Descrizione del team e delle proprie risorse e competenze;

   Il team, costituito all'interno del presidio del Centro Servizi TIX (Tuscany Internet eXchange) di Regione Toscana, è composto da figure con competenze specifiche in ambito applicativo, sistemistico e di rete.

3. Descrizione dei bisogni che si intende soddisfare;

   - Mantenere adeguati livelli di sicurezza delle componenti hardware/software utilizzate per erogare servizi TIX, siano esse risorse IAAS, PAAS, SAAS, tramite operazioni periodiche di VAPT (Vulnerability Assessment and Penetration Test) con consegna ai capiprogetto responsabili delle evidenze emerse e delle remediation da adottare, effettuando nuovi controlli nel tempo per verificare l'avvenuta esecuzione delle remediation consigliate

   - applicare le indicazioni contenute nel CSF ("Framework Nazionale per la Cyber Security") pubblicato dal CIS-Sapienza a febbraio 2016, con particolare rilievo per quelli segnalati da AgID nel documento "Misure minime di sicurezza ICT per le pubbliche amministrazioni del 26 aprile 2016 (Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015)", e successivi aggiornamenti emessi con la CIRCOLARE AGID del 17 marzo

2017, n. 1/2017 Misure minime di sicurezza ICT per le pubbliche amministrazioni.

4. Descrizione dei destinatari della misura;

   Gestori delle risorse attivate sulle infrastrutture TIX, siano essi il presidio stesso (paas, saas) o fornitori terzi (iaas), dirigenti responsabili dei sistemi informativi ospitati, capiprogetto di riferimento;

5. Descrizione della tecnologia adottata;

   - firewall con funzioni di geolocalizzazione,
   - bilanciatori con funzionalità web application firewall,
   - vulnerability assessment e penetration test periodici
   - advanced threat protection
   - SIEM
   - continuous integration (tra cui verifica delle regole OWASP Top 10) per il software di proprietà dell'Amministrazione prodotto da fornitori terzi
   - laboratorio per lo studio delle app mobile su android, iOS, windows phone, con particolare riferimento alla persistenza di dati sensibili sugli smartphone
   - piattaforma per la correlazione di eventi durante l'esecuzione di applicazioni web con riporto di anomalie su sistemi di monitoraggio
   - trattamento log delle componenti middleware su piattaforme hortonworks

6. Indicazione dei valori economici in gioco (costi, risparmi ipotizzati, investimenti necessari);

   L'effort derivato dalle necessarie figure professionali per l'esecuzione dei vari work package VAPT è ridotto per l'utilizzo di figure professionali già comprese nell'accordo quadro attivato per il system management del presidio del centro servizi TIX.

   Nell'acquisizione di componenti infrastrutturali viene data importanza e preferenza a quelle componenti comprensive di funzionalità rivolte alla sicurezza: ad esempio, durante l'iter per il necessario cambio di bilanciatori, causa obsolescenza, è stata data preferenza a modelli di bilanciatori comprensivi di funzionalità di web application firewall.

   La tendenza è quella di utilizzare, ove possibile, tecnologia opensource, non legata quindi a meccanismi di licensing.

   Si configurano ulteriori investimenti per il codice sorgente di proprieta' dell'Amministrazione per la risoluzione delle remediation consigliate dopo i processi di controllo attraverso la piattaforma di continuous integration.

7. Tempi di progetto.

   Progetto iniziato a fine 2015;

   tecnologie attivate nel 2016;

   in corso: analisi del grado di applicazione degli aggiornamenti emessi con la CIRCOLARE AGID del 17 marzo 2017, n. 1/2017 Misure minime di sicurezza ICT per le pubbliche amministrazioni.

   L'analisi è in relazione a due ambiti:

   - Ambito TIX

     le misure analizzate risultano in gran parte già attuate od in corso di applicazione, anche grazie a quanto già realizzato negli anni precedenti per l'ottenimento ed il mantenimento della certificazione ISO/IEC 27001.

- Ambito altri asset ICT di Regione Toscana

  gli asset fissi e mobili che costituiscono l’informatica individuale dei dipendenti dell’Amministrazione

  area dello sviluppo e della conduzione delle applicazioni che interessano vari ambiti (Sanità, Bilancio, Territorio, Supporto alle Decisioni, Statistica …)