Webinar Infosecurity

Di seguito una raccolta di domande pervenute durante i webinar, e le relative risposte.

• *Cosa è un **CERT** e quali attività realizza generalmente?*
I CERT sono organizzazioni incaricate di raccogliere ed analizzare segnalazioni di incidenti informatici e potenziali vulnerabilità nei software, e di renderle disponibili al pubblico.

• *Quali aspetti principali dovrebbero essere garantiti in merito alla protezione delle informazioni da parte di potenziali cyber-attacchi?*
Protezione perimetrale delle reti
Gestione e governo degli accessi alle informazioni
Protezione crittografica dei dati e delle informazioni
Modelli procedurali di gestione consolidati (gestione degli incidenti…)

• *Cosa si intende per sicurezza perimetrale ?*
Si intende l'adozione di misure di natura tecnica, supportate da approcci di natura organizzativa e procedurale, volti a gestire il rischio di intrusioni di soggetti non autorizzati, agendo a livello di rete informatica (tramite dispositivi quali Firewall, …)

• *Cosa si intende per **IoT** (Internet Of Things)?*
Si intende il trend tecnologico per cui dispositivi di varia natura, tradizionalmente non connessi alla rete dati Internet, sono invece attualmente collegati a tali reti dati (e.g. Smartmeter, smartgrid, elettrodomestici intelligenti, …)

• *Quali attività realizza un Security Operation Center (**SOC**)?*
Un SOC è costituito da un insieme di tecnologie, di processi e di competenze specifiche in ambito Sicurezza dei Sistemi informativi. Può essere interno o esterno alle organizzazioni, nel secondo caso si parla di "SOC gestito".

• *Cosa si intende per Cyber Security?*
La Cyber Security è la disciplina che provvede a proteggere tutti quegli asset (materiali e immateriali) che possono essere colpiti tramite un uso malevolo o improprio dell'ICT. In questo senso la Cyber Security si differenzia dall'Information Security in quanto protegge, oltre alle informazioni, anche altri asset quali la reputazione, il funzionamento dei processi di business, ed in casi estremi anche la vita delle persone.

• *Cosa si intende per Cyber Crime ?*
Crimine condotto tramite strumenti informatici (ma non necessariamente solo informatico), sia contro risorse informatiche che, spesso, contro altri tipi di risorse, che vengono raggiunte tramite l'ICT.

• *Cosa si intende per Cyber Risk ?*
Rischio specifico che discende da minacce di tipo "cyber".

• *Cosa si intende per Cyber attacco?*
Attività malevola volta a colpire asset materiali ed immateriali tramite l'uso malevolo dell'ICT.

• *Dato per assodato che una struttura IT minimamente strutturata per il perimetro interno provveda ad aggiornamenti sistematici e programmati di firmware, apparati, update S.O. di devices e servers, applicativi, utilizzo di antivirus centralizzati, firewall (fisici o software), gestione degli account e delle password e quant'altro come gestire e valutare aspetti dei "massimi sistemi"?*
La normativa ha come razionale la riduzione della spesa corrente e dei centri di costo (spingendo le PAL a consolidare le infrastrutture e consorziarsi per la gestione dell'ICT), e non si applica agli investimenti in innovazione, tra i quali quelli di sicurezza. A nostro avviso, più che pensare ad una riduzione delle risorse, è necessario ragionare in termini di una diversa allocazione delle stesse nell'ottica di ottimizzare gli aspetti economico finanziari ed organizzativi, per esempio tramite l'impiego del cloud, l'attivazione di servizi gestiti, (di sicurezza e non), forniti da outsourcers, etc.

• *Esiste un elenco dei CERT territoriali già attivi? Sarebbe molto interessante, data la variegata composizione della pa locale, avere una regia relativa alla dimensione territoriale del Cert. A parte le difficoltà relative all'SPC, a*

maggior ragione se ci sono i fondi europei, andrebbe raccordato un intervento complessivo proponendo un servizio omogeneo a tutti gli enti, anche a quelli di minima dimensione.
Non esiste un elenco ufficiale di CERT territoriali attivi o in fase di definizione. In questa fase alcuni strutture (universitarie, o private) stanno sperimentando strumenti utili ad implementare CERT territoriali, collaborando con AgId

• *Nel caso in cui la firma sia urgentissima (TSO per un comune) ma la firma digitale non funziona come si procede? Stiamo pensando a far firmare su carta ma non sappiamo come gestirlo nel protocollo, visto che non è firma digitale*
In caso di mancato funzionamento della firma digitale bisogna prevedere procedure operative di emergenza.
In particolare l'art. 63 del D.P.R. 28 dicembre 2000, n. 445 disciplina il registro di emergenza per le operazioni di protocollo ogni qualvolta per cause tecniche non sia possibile utilizzare la normale procedura informatica.
In una fase successiva, il documento cartaceo prodotto in emergenza potrà essere dematerializzato.
Si ricorda che ai sensi dell'art. 23 ter comma 3 del CAD, le copie su supporto informatico di documenti formati dalla pubblica amministrazione in origine su supporto analogico hanno il medesimo valore giuridico, ad ogni effetto di legge, degli originali da cui sono tratte, se la loro conformità all'originale è assicurata dal funzionario a ciò delegato nell'ambito
dell'ordinamento proprio dell'amministrazione di appartenenza,

• *Il Responsabile della gestione documentale deve essere un apicale?*
Deve essere un dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione
dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445.

• *Un comune deve accreditarsi per fare l'archiviazione in proprio?*
No, l'accreditamento è richiesto per le società che offrano servizi di conservazione verso la PA.

• *Vorrei sapere come comportarsi nei documenti nativamente digitali con la data del documento. Attualmente non la inseriamo ma vale il certificato delle firme.*
Nel documento informatico immodificabile deve essere presente il riferimento temporale.
Nel D.p.c.m. 13 novembre 2014 si definisce riferimento temporale l'informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento.
Frequentemente si considera come riferimento temporale la data presente nel certificato di firma.

• *In un comune di medie dimensioni, il responsabile dei sistemi informativi può non corrispondere al responsabile della sicurezza?*
La segregazione dei due ruoli dovrebbe essere definita tenendo in considerazione un approccio proporzionale.
Laddove pertanto le risorse dedicate all'IT siano ragionevolmente elevate >10-12 risorse è bene che ci siano esplicite responsabilità di sicurezza attribuite a particolari referenti. Le indicazioni normative non sono però deterministiche su questo caso.

• *Quali possono essere i compiti di eventuali vicari del Responsabile della gestione documentale?*
Il vicario svolge i medesimi compiti del responsabile della gestione documentale nei casi di sua vacanza, assenza o impedimento.