Competenze in cybersecurity: articolazione e percorso verso la certificazione delle professionalità

Paolo Atzeni

ACN, Struttura di Missione Capacità e Competenze

Professore di Ingegneria Informatica in aspettativa, Università Roma Tre

Le competenze in cybersecurity

- Problematiche analoghe a quelle relative all'innovazione tecnologia e alla trasformazione digitale in generale
  - La cybersecurity interessa tutte le persone e tutte le attività, così come le tecnologie informatiche possono essere applicate in ogni contesto
- Come certamente discusso nei precedenti webinar la cybersecurity
  - è un requisito essenziale dei sistemi moderni (e non solo dei sistemi, ma anche delle infrastrutture)
  - non può essere separata dallo sviluppo e dalla gestione perché non è qualcosa che può essere aggiunto a posteriori

Competenze informatiche

- Dirigenti, quadri, impiegati esecutivi sono tutti interessati alle tecnologie informatiche (IT), in modalità diversa a seconda delle responsabilità
  - esecutivi
    - lavorano con le tecnologie
  - quadri
    - coordinano specifiche attività, supportate dall'IT
  - dirigenti
    - governano insiemi di attività, supportate dall'IT

Competenze informatiche (2)

- Ciascuno deve avere le competenze necessarie per interagire con i propri interlocutori
  - gli esecutivi
    - debbono saper utilizzare gli strumenti
  - i quadri
    - debbono conoscere (definire, modificare) i processi amminstrativi e poter interagire con gli specialisti informatici (che realizzano o gestiscono i sistemi)
  - i dirigenti
    - debbono conoscere le potenzialità delle tecnologie informatiche e le opportunità che esse offrono e poter interagire con gli specialisti informatici di livello più alto per valutare le iniziative da intraprendere

Osservazione importante

- La funzione IT è di supporto, ma contribuisce alla strategia dell'ente e le sue iniziative vengono definite e programmate con interazione bidirezionale
- Il rapporto fra i vertici dell'ente (DG o simili) e i responsabili informatici (CIO o simili) deve essere molto stretto (e il CIO deve essere ad un livello non troppo lontano dal vertice)
- Lo stesso rapporto deve permanere ai vari livelli, fino all'operatività
- Le attività possono (e talvolta debbono) essere affidate all'esterno, ma senza perderne il governo e il controllo (sempre ai vari livelli)

E per la cybersecurity?

- Molte similitudini e qualche differenza
  - Il responsabile (ad esempio CISO: Chief Information Security Officer)
    - deve essere molto vicino al vertice dell'ente (che deve essere totalmente consapevole, delegando l'attività ma, nella sostanza, mantenendo la responsabilità)
      - nella funzione informatica
        - e coincidere con il relativo vertice
        - o comunque essere molto vicino
      - o in una funzione "sorella" (soprattutto se ci sono significative componenti fisiche)
    - può essere
      - uno specialista di cybersecurity
      - un esperto IT generalista
      - una figura non IT

E per la cybersecurity? (2)

- L’interazione persiste a tutti i livelli
  - la funzione IT può
    - gestire direttamente la cybersecurity
      - con personale specializzato o
      - con personale IT con competenze di cybersecurity
    - gestire la cybersecurity con il supporto di una funzione ad-hoc (interna o esternalizzata)
      - ma comunque l’interazione deve essere stretta
  - gli "utenti" (dirigenti, funzionari, operativi) debbono comunque tenere presente le esigenze e gli obiettivi di cybersecurity, senza poter assumere che se ne occupi qualcun altro

Quali figure per la cybersecurity?

- Diverse coordinate
  - livello di responsabilità
    - ad esempio impiegato, quadro, dirigente
  - tipo di attività
    - nel dominio applicativo, nell'IT, nella sicurezza in senso stretto

Figure per la cybesecurity

- **ENISA** (European Union Agency for Cybersecurity):
  - rapporto sulla (scarsa) disponibilità di competenze (dicembre 2019)
  - quadro di riferimento sulle competenze (**ECSF**: European Cybersecurity Skills Framework), in preparazione
    - bozza 5 aprile 2022
    - rilascio previsto a settembre 2022

Osservazione importante dal rapporto ENISA

- Il mercato del lavoro nel settore della cybersecurity non è ancora ben definito e quindi è molto dinamico
- Le specifiche delle varie posizioni dipendono molto dalle dimensioni dell'organizzazione e dal settore
  - PMI non specializzate in cybersecurity
    - personale IT generalista con alcune competenze in cybersecurity
  - grandi aziende e aziende focalizzate sulla cybersecurity
    - personale specializzato in cybersecurity, anzi in specifiche sottodiscipline della cybersecurity

Figure specialistiche previste in ECSF

- Chief Information Security Officer (CISO)
- Cyber Incident Responder
- Cyber Legal, Policy & Compliance Officer
- Cyber Threat Intelligence Specialist
- Cybersecurity Architect
- Cybersecurity Auditor
- Cybersecurity Educator
- Cybersecurity Implementer
- Cybersecurity Researcher
- Cybersecurity Risk Manager
- Digital Forensics Investigator
- Penetration Tester

Figure specialistiche previste in ECSF

- Chief Information Security Officer (CISO)
- Cyber Incident Responder
- Cyber Legal, Policy & Compliance Officer
- Cyber Threat Intelligence Specialist
- Cybersecurity Architect
- Cybersecurity Auditor
- Cybersecurity Educator
- Cybersecurity Implementer
- Cybersecurity Researcher
- Cybersecurity Risk Manager
- Digital Forensics Investigator
- Penetration Tester

- Manager tecnico
- Tecnico specializzato
- Tecnico specializzato
- Tecnico specializzato
- Tecnico specializzato
- Tecnico specializzato
- Formatore tecnico
- Tecnico
- Ricercatore
- Tecnico specializzato
- Tecnico (specializzato)
- Tecnico

Non servono solo le figure specialistiche …

- … perché
  - c’è carenza ("skill shortage")
  - molte realtà non possono permettersi posizioni dedicate

Carenza di personale specializzato

- Cause, sempre dal rapporto ENISA
  - novità e immaturità della cybersecurity come professione
  - mancanza di laureati in discipline scientifiche, tecnologiche, ingegneristiche e matematiche (STEM)
  - scarsa consapevolezza della cybersecurity come opzione di carriera.
  - mancanza di formazione continua e ricorrente, necessaria per garantire l'aggiornamento sui temi di cybersecurity del personale di con background generale

Come rispondere a questa esigenza

- Nella **Strategia Nazionale di Cybersicurezza**
  - fattore abilitante **formazione**
    - promozione dell'informatica come disciplina (dalla scuola primaria all'università)
    - promozione dei percorsi scientifici e tecnologici (discipline STEM) e più specificamente dei percorsi in cybersecurity, nella scuola superiore, negli ITS, nei vari livelli universitari
    - aggiornamento della didattica e del corpo docente, ancora a tutti i livelli
    - incentivazione della formazione specialistica e dell'aggiornamento professionale
    - definizione di un sistema di certificazione
    - pianificazione e realizzazione di un sistemi di percorsi di formazione per non specialisti
    - potenziamento delle capacità di cyber diplomacy

Come rispondere a questa esigenza (2)

- Nell'**Implementazione della Strategia**, 12 misure
  59. Percorsi formativi a tutti i livelli
  60. ITS dedicati alla cybersecurity
  61. Sistema di certificazione
  62. Strumenti di formazione e sensibilizzazione on-line
  63. Fondi per la formazione professionale
  64. Incentivi per le start-up
  65. Iniziative e competizioni mirate anche alla riduzione del gender gap
  66. Iniziative per l'orientamento e l'inserimento nel mondo del lavoro
  67. Programmi di scambio internazionali, universitari e professionali, mirati anche alla riduzione del gender gap
  68. Formazione per le figure impegnate nel contrasto alla criminalità informatica
  69. Formazione del personale diplomatico alla cyber diplomacy
  70. Aggiornamento professionale a tutti i livelli

Un inciso importante

- Strategiche le azioni relative a formazione professionale e ITS:
  59. Percorsi formativi a tutti i livelli
  60. ITS dedicati alla cybersecurity
- Motivazione: ci sono molti livelli di formazione
  - il nostro paese ha pochi laureati (soprattutto STEM)
    - aumentare il numero di laureati non è semplice
  - più precisamente, il paese ha numeri bassi nella somma dei dei numeri di post diplomati e laureati
    - è possibile aumentare il numero dei post diplomati (e dei laureati triennali dei corsi professionalizzanti)
    - con iniziative concrete e senza studi formali propedeutici (causa di molti abbandoni nei corsi universitari)
  - ci sono molte posizioni che potrebbero essere adatte anche a non laureati (e che i laureati non accettano facilmente)

Certificazione

- Misura #61:
  - Sviluppare un sistema nazionale di certificazione dell'apprendimento e dell'acquisizione di specifiche professionalità, non solo tecniche, sia a livello di istruzione secondaria di secondo grado, sia a livello universitario e professionale. L'ACN mantiene una lista dei percorsi di formazione, approvati dalla stessa Agenzia, al termine dei quali il discente consegue, oltre al titolo di studio/professionale, la relativa certificazione

Certificazione

- La sfida è enorme
  - certificazioni a più livelli
  - professionalità non solo tecniche

Esperienze di altri paesi (rapporto ENISA)

- Sono relative ai percorsi specialistici, a livello universitario
- Criteri generali
  - Focus e massa critica di contenuti e attività cyber
  - Curriculum strutturato
  - Qualità della docenza (eventualmente anche da industria)
  - Multidisciplinarità
  - Attività esterne e collaborazioni con l'ecosistema cyber
  - Inserimento nel mondo del lavoro

Ancora spunti dal rapporto ENISA

- **Adequate amount of taught courses and activities that are specific to cybersecurity**. This is done to differentiate courses that are in cybersecurity (or computer science degrees with a clear focus on cybersecurity) from IT courses that could claim to provide some sort of cybersecurity education but not enough to form well-rounded cybersecurity graduates.
- Certification is typically awarded to those institutions that can show in great detail **how cybersecurity education is provided**. For example, national authorities often inquire about the structure of the curriculum and if more practical training is included. Moreover, a number of certification processes ask directly about the kind of examinations students undergo, including for example how students do their dissertations, what courses take place to increase students' academic skills, how much time students spend on hands-on activities and if students are encouraged to attend cybersecurity competitions.
- A lot of importance is placed on the **quality of the faculty**, meaning that national authorities request biographies and curricula vitae of lecturers. Academic institutions are often asked to clarify the nature of the cybersecurity research that faculty is engaged in and if at least part of the faculty has an industry background.
- Degrees that have a **broader interdisciplinary focus** have more chance of being certified. For example, topics that are not solely technical are strongly encouraged, such as legal courses on data protection.

Tipi di certificazioni (o accreditamenti)?

- Corsi in cybersecurity
  - Formazione professionale
  - ITS
  - Corsi di Laurea
  - Corsi di Laurea Magistrale
  - Corsi di dottorato (o forse singoli titoli)
- Competenze in cybersecurity per specialisti IT
  - A ciascuno dei livelli
- Competenze in cybersecurity per "utenti"
  - A tutti i livelli professionali (dall’operatore al dirigente)

Conclusioni

- Un quadro articolato
- Un lavoro complesso che richiederà un coinvolgimento ampio di esperienze e competenze, amministrative, tecniche e didattiche
- Prossime attività
  - piano dettagliato entro settembre
    - interazione con amministrazioni centrali e periferiche, atenei e associazioni accademiche, imprese e associazioni imprenditoriali
  - prime iniziative immediate
    - formazione professionale, accordi con Regioni (stipulato con il Lazio, altri in discussione)
    - ITS, nuova legge, discussioni in corso per sperimentazioni in alcune Regioni (Emilia Romagna, Umbria, Liguria, Puglia, Lombardia)