Cybersecurity e protezione dei dati: il ruolo della certificazione accreditata

Alessandro Armando
Università degli Studi di Genova
Vice Direttore Cybersecurity National Lab

Università di Genova

CYBERSECURITY NATIONAL LAB

Introduzione

Certificazione e Accreditamento come "*Trust Enablers*"

- **Cybersicurezza** e **fiducia** (*trust*) sono concetti intimamente correlati.
- Le garanzie di cybersicurezza di un sistema complesso **assumono** che i componenti soddisfino determinati **requisiti di sicurezza**.
- È dunque fondamentale poter identificare le componenti di cui potersi **fidare** e avvalersi.
- Altrettanto importante è poter **verificare nel tempo** le basi per la **fiducia**.
- Certificazione e accreditamento sono come elementi fondamentali della catena di fiducia che permette di **costruire sistemi robusti**, **identificare responsabilità**, **misurare** e **verificare** le **garanzie di sicurezza** raggiunte.

Certificazione e Accreditamento come "*Trust Enablers*"

- Un prodotto non certificato è una potenziale sorgente di insicurezza.
- Tale rischio si attenua se il prodotto è certificato in accordo ad uno standard riconosciuto, ma rimangono aperti dei quesiti:
  - Quale soggetto ha certificato il prodotto?
  - Che **garanzie di fiducia** esistono rispetto a questo soggetto?
- L'accreditamento risponde a questi quesiti, attraverso la **migrazione della fiducia verso l'ente di accreditamento**, che per ruolo e responsabilità dovrà avere i connotati adeguati per potere offrire tale fiducia.
- Accreditamento significa **vigilanza**, **monitoraggio**, **implementazione di meccanismi di verifica pubblica**, **uniformità** ed **interoperabilità**.

Standard e Norme

Conformità rispetto a standard e norme non significa solo **tutela rispetto a sanzioni o responsabilità**, ma anche **capacità**

- di **definizione e pianificazione delle strategie** di cybersicurezza e delle azioni conseguenti in modo corretto e completo,
- di **monitorare l'adozione delle strategie** in ogni fase, misurandone il grado di attuazione e la loro efficacia, nonché
- di **poter dimostrare la maturità delle proprie strategie** di fronte a terzi.

Certificazione e l'**accreditamento** giocano un ruolo fondamentale.

Servizi accreditati

- I servizi accreditati sono servizi di **valutazione della conformità** che, assicurano
  - il **rispetto di norme** riconosciute sia a livello nazionale che internazionale
  - offrono **garanzie sulla qualità e sulla sicurezza** dei prodotti e dei servizi.
- Esempi: certificazioni, ispezioni e verifiche svolti dagli organismi e dai laboratori accreditati
- Il beneficio apportato dai servizi accreditati è importante in una varietà di ambiti, ma diventa cruciale in un ambito sensibile quale quello della cybersicurezza.

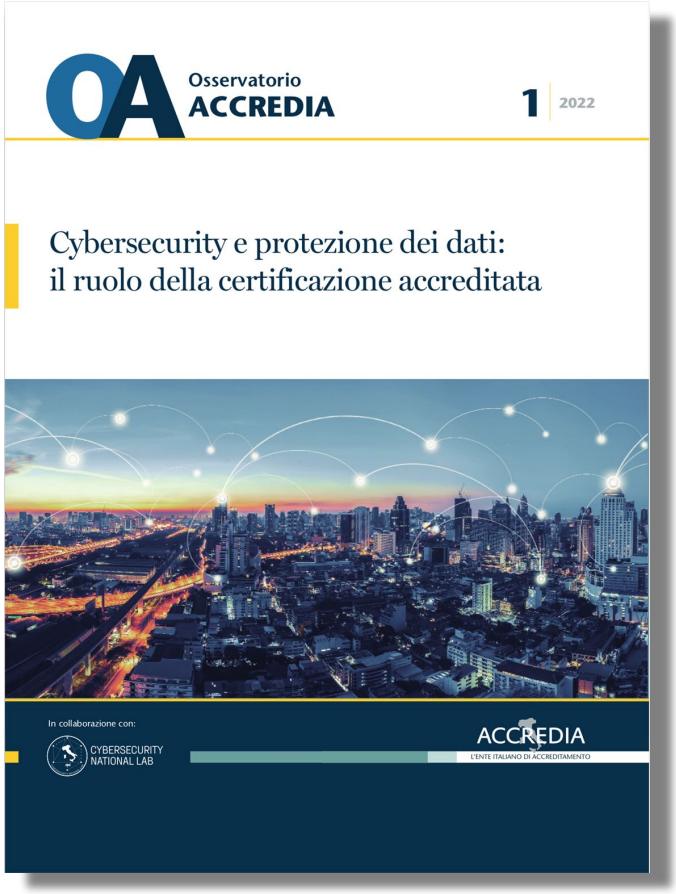
Servizi accreditati di cybersicurezza

Giocano un ruolo centrale

- nell'offrire **garanzie circa il rispetto di requisiti di sicurezza fondamentali** quali
  - la **tutela della privacy** e
  - la **protezione dell'erogazione dei servizi essenziali** dalla minaccia cyber.
- nel **costruire relazioni di "fiducia" tra produttori e consumatori di prodotti e servizi digitali**.

Struttura del Rapporto

1. Introduzione
2. Analisi del Panorama Normativo/Regolatorio
3. Analisi dei servizi accreditati per la cybersicurezza
4. Casi di Studio
5. Attività sul Campo
6. Prospettive dei servizi accreditati di cybersicurezza
7. Considerazioni Finali



Il Gruppo di Lavoro

ACCREDIA

- Riccardo Bianconi
- Amerigo Cancellieri
- Gianluca Di Giulio
- Lorenza Guglielmi
- Alessandro Nisi
- Guglielmo Tozzi
- Pietro Vitaliano
- Alessandra Zacchetti

Cybersecurity National Lab

- Alessandro Armando
- Francesco Buccafurri
- Fabio De Rosa
- Giorgio Giacinto
- Paolo Prinetto
- Leonardo Querzoni
- Luca Verderame

Il Panorama Normativo/Regolatorio

Capitolo diretto da:

Francesco Buccafurri

Università Mediterranea di Reggio Calabria
Vice-direttore del Cybersecurity National Lab

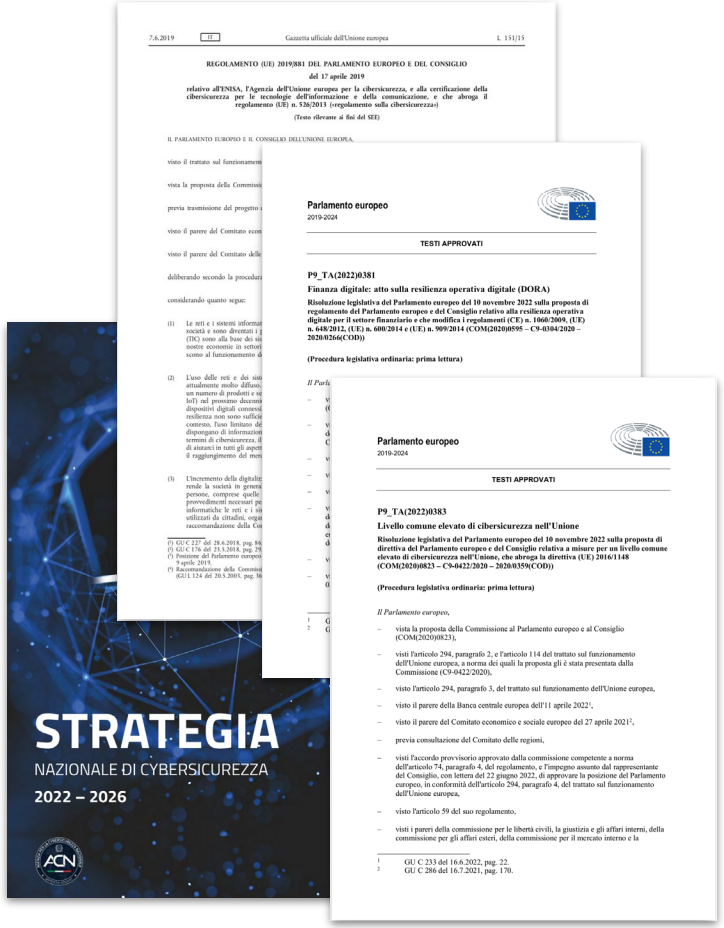
Fabio De Rosa

Cybersecurity National Lab

CYBERSECURITY NATIONAL LAB

Il Panorama normativo/regolatorio

- EU – Cybersecurity Act
- Infrastrutture Critiche – NIS e NIS2
- IT – Perimetro di Sicurezza Nazionale Cibernetica
- Strategia Nazionale di Cybersicurezza
- Privacy – GDPR
- Direttive per specifici domini
  - Regolamento UE 910/2014 (eIDAS)
  - Schema di certificazione europea dei servizi cloud (EUCS)
- Settore Finanziario
  - PSD2
  - Digital Operational Resilience



Strategia Nazionale di Cybersicurezza: gli Strumenti

IL PIANO NAZIONALE DI RIPRESA E RESILIENZA: INVESTIMENTO 1.5 “CYBERSECURITY”

01 **174 M€**

SERVIZI CYBER NAZIONALI

Contribuendo all’attivazione e piena operatività dell’Agenzia, le reti e i servizi che saranno realizzati potenzieranno le capacità nazionali di prevenzione, monitoraggio, risposta e mitigazione di minacce cyber.

02 **301.7 M€**

INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER PER LA PA

Le capacità cyber della PA sono un elemento fondante per una transizione digitale sicura del Paese, assicurando quindi adeguati livelli di sicurezza per i dati e i servizi dei cittadini.

03 **147.3 M€**

LABORATORI DI SCRUTINIO E CERTIFICAZIONE TECNOLOGICA

Il raggiungimento di un’autonomia tecnologica nazionale passa necessariamente anche dal potenziamento delle capacità nazionali di scrutinio e certificazione tecnologica, in stretta collaborazione con il mondo privato dell’industria e dell’accademia.

Strategia Nazionale di Cybersicurezza: gli Obiettivi

1. OBIETTIVO PROTEZIONE

A. il **potenziamento delle capacità del Centro di Valutazione e Certificazione Nazionale (CVCN)** dell'Agenzia per la Cybersicurezza Nazionale e, negli ambiti di competenza, dei **Centri di Valutazione (CV)** del Ministero dell'Interno e della Difesa, nonché l'integrazione con una rete di Laboratori Accreditati di Prova, permetterà di sviluppare capacità nazionali di valutazione delle vulnerabilità di tecnologie avanzate a servizio degli asset più critici del Paese;

B. la **definizione ed il mantenimento di un quadro giuridico nazionale aggiornato e coerente** in materia di cybersicurezza, che tenga conto degli orientamenti e degli sviluppi in ambito europeo ed internazionale. Tale impianto non ricomprende solamente il livello normativo, quanto anche l'insieme di linee guida, schemi di certificazione e policy settoriali rivolte ai soggetti pubblici e agli operatori privati. In tale contesto, assume rilevanza primaria:

- il *supporto allo sviluppo di schemi di certificazione e standard europei e internazionali* in materia di cybersicurezza;
- la *promozione dell'utilizzo di schemi di certificazione europea in materia di cybersicurezza,* da parte delle imprese italiane specializzate, al fine di conseguire un vantaggio competitivo sul mercato;

Strategia Nazionale di Cybersicurezza: gli Obiettivi

3. OBIETTIVO SVILUPPO

- la realizzazione di un *sistema nazionale di certificazione di tali professionalità* (sia in ambito scolastico/accademico che lavorativo), mediante l'attivazione di percorsi di formazione ad hoc approvati dall'ACN;

Strategia Nazionale di Cybersicurezza: Implementazione

PROTEZIONE | Scrutinio tecnologico

Misura #1

Rafforzare il sistema di scrutinio tecnologico nazionale a supporto della sicurezza della supply chain delle particolari categorie di asset rientranti nel Perimetro e per l'adozione di schemi di certificazione europea di cybersecurity, anche mediante l'accreditamento di laboratori di valutazione pubblico/privati.

Attori responsabili
ACN

Altri soggetti interessati
Min. Interno, Min. Difesa, Operatori privati

Strategia Nazionale di Cybersicurezza: Implementazione

Definizione e mantenimento di un quadro giuridico nazionale aggiornato e coerente

Misura #5

Supportare lo sviluppo, valutandone l'adeguatezza in termini di sicurezza nazionale, degli schemi di certificazione in materia di cybersicurezza e, in collaborazione con il settore privato, promuoverne l'adozione e l'utilizzo da parte dei fornitori di servizi e delle imprese italiane, favorendo lo sviluppo del tessuto imprenditoriale nazionale specializzato al fine di conseguire un vantaggio competitivo sul mercato.

Attori responsabili
ACN, MITD

Altri soggetti interessati
MiSE,
Associazioni di categoria

Strategia Nazionale di Cybersicurezza: Implementazione

FATTORI ABILITANTI | **Formazione**

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.

Attori responsabili
ACN, Atenei, Ministero dell'Istruzione, MUR

Altri soggetti interessati
Operatori privati, Regioni e Province autonome

Cybersecurity Act

- Introduce un **quadro complessivo di regole che disciplinano gli schemi europei di certificazione della sicurezza informatica**, incluso un framework di base su cui istituire schemi europei per la certificazione.
- Tali schemi di certificazione, da predisporsi per specifiche categorie di prodotti e servizi, comporterà tuttavia che **i certificati rilasciati secondo tali schemi saranno validi e riconosciuti in tutti gli Stati membri**.
- Le aziende interessate potranno presentare domanda di certificazione dei propri prodotti o servizi a specifici organismi accreditati.
- L'utilizzo della certificazione rimarrà tuttavia volontario, a meno che la certificazione venga espressamente richiesta per determinate categorie di prodotti o servizi da specifiche norme di settore.
- Verso un **mercato europeo della certificazione della sicurezza informatica di prodotti ICT e servizi digitali**.

NIS2

Articolo 7 - Strategia nazionale per la cibersicurezza

[...]

2. Nell'ambito della strategia nazionale per la cibersicurezza, gli Stati membri adottano in particolare misure strategiche riguardanti:

a) la **cibersicurezza nella catena di approvvigionamento dei prodotti e dei servizi TIC** utilizzati da soggetti per la fornitura dei loro servizi;
b) l'inclusione e la definizione di requisiti concernenti la cibersicurezza per i prodotti e i servizi TIC negli appalti pubblici, compresi **i requisiti relativi alla certificazione della cibersicurezza**, alla cifratura e l'utilizzo di prodotti di cibersicurezza open source

NIS2

Articolo 24 - Uso dei sistemi europei di certificazione della cibersicurezza

1. "[...] gli Stati membri possono imporre ai soggetti essenziali e importanti di utilizzare determinati prodotti TIC, servizi TIC e processi TIC, sviluppati dal soggetto essenziale o importante o acquistati da terze parti, **che siano certificati nell'ambito dei sistemi europei di certificazione della cibersicurezza** [...]. Inoltre, gli Stati membri incoraggiano i soggetti essenziali e importanti a utilizzare servizi fiduciari qualificati."
2. "[...] categorie di soggetti essenziali e importanti **sono tenute a utilizzare determinati prodotti TIC, servizi TIC e processi TIC certificati o a ottenere un certificato nell'ambito di un sistema europeo di certificazione della cibersicurezza** [...]"

Settore finanziario & Cybersicurezza

- Circolare n. 285 del 17/12/2013
- Payment Service Directive 2 (2015/2366/EU)
- EBA Guidelines on ICT and security risk management - EBA/GL/2019/04
- EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02)
- Revised Guidelines on major incident reporting under PSD2 (EBA/GL/2021/03)
- Cyber Resilience Oversight Expectations for financial market infrastructures
- **Digital Operation Resilience Act (DORA)**

Digital Operation Resilience Act (DORA)

Articolo 27 - **Requisiti per i soggetto incaricato dello svolgimento dei test per lo svolgimento dei TLPT**

1. Per lo svolgimento dei **test di penetrazione basati su minacce**, le entità finanziarie ricorrono unicamente a soggetto incaricato dello svolgimento dei test che:

a) possano vantare il più alto grado di idoneità e reputazione;

b) possiedano capacità tecniche e organizzative e dimostrino esperienza specifica nel campo delle analisi delle minacce, dei test di penetrazione e dei test red team;

c) siano **certificati da un ente di accreditamento in uno Stato membro** o rispettino codici formali di condotta o quadri etici.

[...]

Servizi accreditati per la cybersicurezza

Capitolo diretto da:

Giorgio Giacinto
Università degli Studi di Cagliari
Cybersecurity National Lab

UNIVERSITÀ DEGLI STUDI DI CAGLIARI

CYBERSECURITY NATIONAL LAB

Servizi accreditati per la cybersicurezza

1. Accreditamento - Regolamento (Ce) N. 765/2008
2. Sistemi di Gestione della Sicurezza delle Informazioni - ISO/IEC 27001, ISO/IEC 27XXX
3. Ispezioni e Verifiche sulla Sicurezza delle Informazioni e Cybersecurity
4. Vulnerability Assessments
5. Regolamento UE 910_2014 (EIDAS)
6. Data Protection Officer (DPO)

Accreditamento

- La **certificazione** avviene tramite organismi pubblici o privati **accreditati**, ovvero organismi ritenuti **idonei** a effettuare in modo **competente**, **adeguato** e **imparziale** le verifiche di processi e prodotti
- **Accredia** gestisce il processo di accreditamento attraverso il quale si attesta la capacità di un soggetto di rilasciare una o più certificazioni.
- L'accreditamento funge da abilitatore della **fiducia** che il mercato ripone nei **risultati delle valutazioni** di conformità.

Accreditamento: le Fasi

- Domanda di accreditamento
- Esame della documentazione
- Verifiche ispettive in sede
- Delibera dell’accreditamento
- Sorveglianza periodica
- Estensione dell’accreditamento
- Rinnovo dell’accreditamento

Sistemi di gestione della sicurezza delle informazioni (ISMS)

- Norma tecnica **ISO/IEC 27001** aggiornata nel **2022** cui sono collegate norme specifiche nella famiglia **ISO/IEC 27XXX.**
- Obiettivo: **ridurre in modo significativo il livello di rischio**
- Esistono **diversi organismi accreditati** cui rivolgersi per il processo di certificazione. La **scelta** si basa su considerazioni di carattere commerciale e relativo allo specifico settore di attività in cui l'organismo di certificazione è competente.
- Un **organismo certificato** è sottoposto a **sorveglianza** (audit) **periodica** con cadenza di massima annuale per garantire **efficacia degli ISMS nel tempo.**

Ispezioni e verifiche

Gli organismi che effettuano **ispezioni e verifiche sulla sicurezza delle informazioni e cybersicurezza** devono sottoporsi alla **procedura di accreditamento**.

Accredia verifica (UNI CEI EN ISO/IEC 17020):

- **competenza**, **imparzialità** e **riservatezza** del personale coinvolto nelle attività ispettive
- **conformità delle procedure** di ispezione alle norme
- **verifiche in accompagnamento** in cui gli ispettori di Accredia **osservano il comportamento dell'ispettore** dell'organismo presso le varie organizzazioni.

Vulnerability Assessment (VA)

Attività di verifica della presenza di **vulnerabilità note** che possono consentire a un soggetto malintenzionato di **ottenere** o **alterare** le **informazioni** o di **bloccare** in tutto o in parte le funzionalità di un sistema.

Un **laboratorio di prova** che voglia accreditarsi per eseguire attività di VA deve:

- predisporre la **documentazione che descrive gli aspetti organizzativi e operativi** delle attività di VA
- sottoporsi a **audit** da parte di **Accredia** per la verifica della **idoneità del personale e delle dotazioni strumentali** per condurre le verifiche sul campo.

Le fasi del Vulnerability Assessment

- **Preparazione**
  Definizione del **perimetro** della verifica (dispositivi, sistemi), tempi e modalità
- **Esecuzione**
  utilizzo di **strumenti automatici o semi-automatici** di verifica
- **Analisi dei risultati**
  relazione con elenchi di minacce note ed eliminazione dei falsi positivi
- **Valutazione dei rischi**
  produzione del rapporto di prova contenente le vulnerabilità riscontrate e le **prescrizioni** e **raccomandazioni** per la mitigazione del rischio
- **Follow-up**
  gestione delle vulnerabilità indicate nel **rapporto di prova**

Casi di Studio

Capitolo diretto da:

Leonardo Querzoni
Sapienza Università di Roma
Cybersecurity National Lab

SAPIENZA
UNIVERSITÀ DI ROMA

CYBERSECURITY
NATIONAL LAB

Obiettivi dell'analisi

A **qualitativa di alcuni casi di studio** relativi a organizzazioni di diversa natura, che hanno intrapreso un percorso di certificazione legato alla cybersicurezza.

Obiettivi dell'analisi:

- comprendere le **motivazioni**;
- identificare le possibili **criticità** nella fase di adeguamento;
- valutare gli **effetti**, diretti ed indiretti, del processo di certificazione da diversi punti di vista.

Analisi limitata a casi di certificazione dell'**Information Security Management System** (ISMS) secondo la norma tecnica **ISO/IEC 27001** e norme collegate.

Casi selezionati

L’analisi è partita dall’**individuazione dei casi di studio**, in numero limitato e in grado di rappresentare realtà differenti da diversi punti di vista: dimensioni, natura, mercato di riferimento, esperienza.

Sono state selezionate **quattro organizzazioni**:

- Gruppo BCC Iccrea
- Poste Italiane
- ATAC S.p.A.
- Notartel

L’indagine è stata svolta attraverso un’**intervista erogata da due esperti del gruppo di lavoro al personale delle organizzazioni selezionate**.
A ciascuna organizzazione è stato chiesto di identificare le persone più adatte a interloquire sul tema (CISO, CIO, o similari).

Questionario

L’intervista è stata svolta basandosi su un **questionario** precedentemente condiviso con le organizzazioni selezionate.

Il questionario, definito in modo specifico per questo studio, consiste in **19 domande suddivise in tre parti**:

- Domande introduttive su **motivazioni e ambito** della certificazione (2)
- Domande sulla complessità affrontata in **fase di adeguamento** (7)
- Domande sugli **effetti della certificazione** (10)

A valle delle interviste, alla luce delle risposte fornite al questionario, è stata svolta un’analisi indirizzata ad individuare gli elementi caratterizzanti le esperienze condivise dalle organizzazioni selezionate.

Considerazioni emerse dai casi di studio

Ciascun caso ha esposto specificità proprie dell'organizzazione e di come questa ha affrontato il percorso di certificazione. Alcune **considerazioni generali**:

- Gli effetti della certificazione sono **apprezzabili in modo completo sul lungo periodo**.
- La certificazione di un ISMS è un **elemento facilitatore per la conformità** rispetto ai numerosi regolamenti che impongono requisiti legati alla cybersecurity.
- L'**approccio risk-based** rappresenta uno dei **valori aggiunti più importanti** acquisiti con l'adozione dell'ISMS, ma anche uno dei **punti critici nella fase di adeguamento** e successivamente di mantenimento della certificazione.

L'analisi ha inoltre permesso di evidenziare alcune **strategie** che risultano efficaci nel processo di certificazione.

Attività sul Campo

Capitolo diretto da:

Luca Verderame
Università degli Studi di Genova
Cybersecurity National Lab

Università di Genova

CYBERSECURITY NATIONAL LAB

Obiettivo dell'Attività sul Campo

- Valutazione del recepimento delle **misure basilari di sicurezza informatica** indotte dal processo di certificazione di Cybersicurezza.
- Esecuzione di una campagna di **Vulnerability Assessment dei servizi web esposti al pubblico** su **campioni di due popolazioni** di organizzazioni private e pubbliche nazionali
  - una dotata di **certificazione per la sicurezza delle informazioni ISO/IEC 27001**
  - l'altra dotata solamente della **certificazione per la qualità ISO 9001.**
- Ispirato alla metodologia utilizzata da CERT-AgID per rilevazione sull'utilizzo del protocollo HTTPS e l'aggiornamento dei CMS nei sistemi della PA.[1]

[1] CERT-AgID. *Secondo monitoraggio dello stato di aggiornamento del protocollo HTTPS e dei CMS sui sistemi della PA*. 2021. https://cert-agid.gov.it/news/secondo-monitoraggio-dello-stato-di-aggiornamento-del-protocollo-https-e-dei-cms-sui-sistemi-della-pa/

Campione Considerato

Valutazione effettuata su due popolazioni di organizzazioni private e pubbliche italiane:

- 50 Aziende certificate ISO/IEC 27001
- 50 Aziende certificate ISO 9001 ma non ISO/IEC 27001

Le due popolazioni sono state ulteriormente classificate in sottocategorie tenendo conto dei seguenti criteri:

- dimensione aziendale (Micro, Piccola, Media e Grande Impresa)
- ripartizione geografica (Nord Ovest, Nord Est, Centro, Sud, Isole)

Metodologia di Analisi

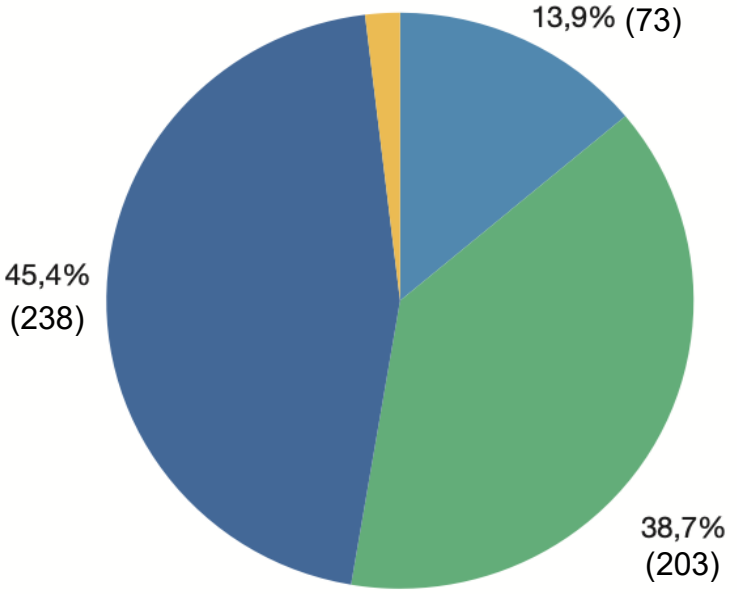
Vulnerability Assessment sui servizi web dei due campioni:

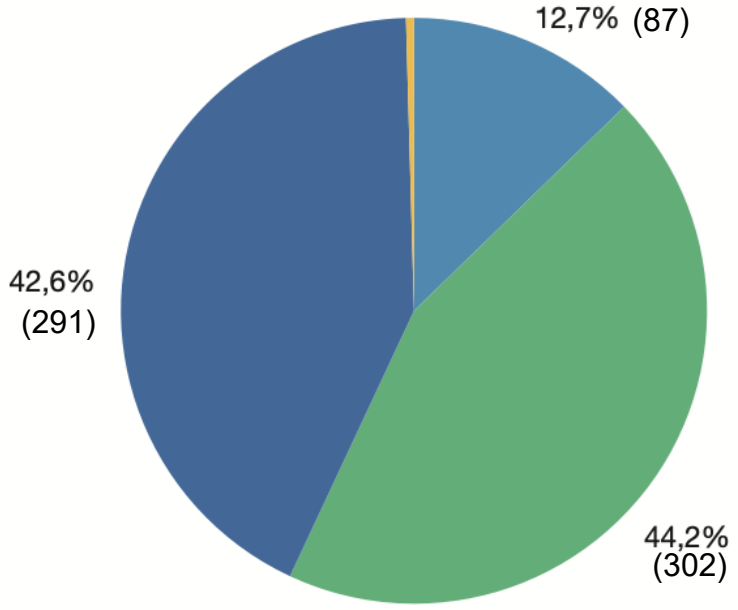
- limitatamente alla superficie pubblica esposta
- in modalità *black box* (nessuna conoscenza pregressa sui sistemi analizzati)
- completamente passivo (no penetration testing)
- tramite strumenti automatici e analisi manuale
- utilizzando metodologie e procedure di analisi allo stato dell'arte:
  - *Open Source Security Testing Methodology*
  - *OWASP Web Application Security Testing Guide*

Categorie di Valutazione

- Servizi esposti, porte aperte, versioni dei software utilizzati, presenza di eventuali vulnerabilità CVE associate alla configurazione individuata
- Utilizzo protocollo di comunicazione sicura HTTPS, validità certificati, utilizzo protocolli non obsoleti/vulnerabili (9 gradi - da A+ a T)
- Utilizzo sistemi di Content Management Systems aggiornati e sicuri (versione CMS, CVE associati)

Risultati: Distribuzione Vulnerabilità Potenziali





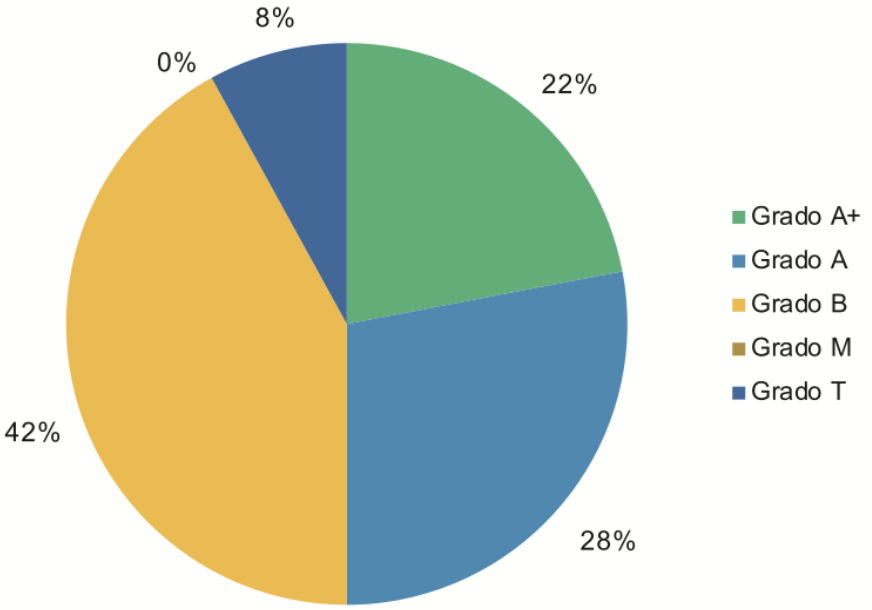
Organizzazioni certificate ISO/IEC 27001

Vulnerabilità Totali: **524**

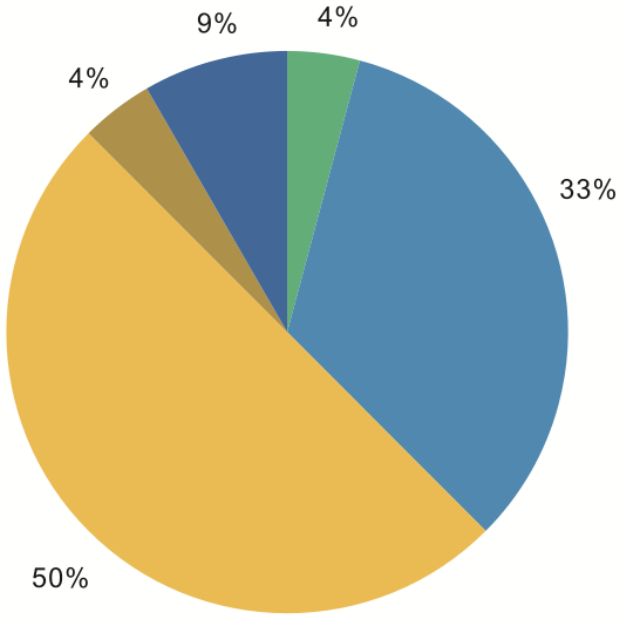
Organizzazioni certificate ISO 9001

Vulnerabilità Totali: **683**

Risultati: Utilizzo sicuro del protocollo HTTPS

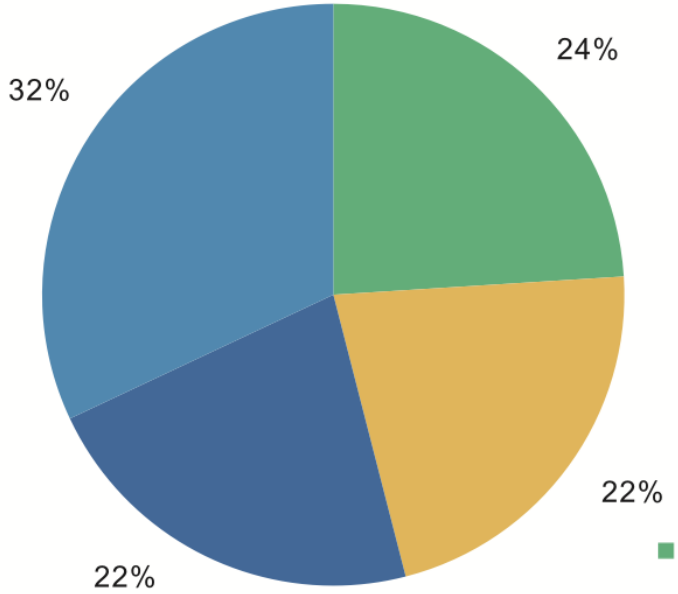


Organizzazioni certificate ISO/IEC 27001

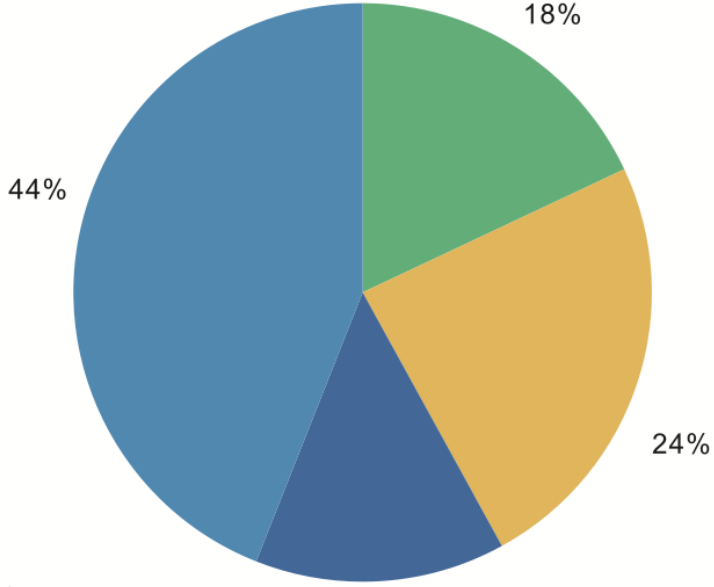


Organizzazioni certificate ISO 9001

Risultati: Analisi utilizzo Content Management System



Organizzazioni certificate ISO/IEC 27001



Organizzazioni certificate ISO 9001

- Versione Aggiornata
- Versione Non Aggiornata
- Versione Non Rilevata
- Nessun CMS Rilevato

Conclusioni dell’Analisi sul Campo

- Le organizzazioni certificate **ISO/IEC 27001** appaiono **globalmente meno suscettibili a gravi vulnerabilità** di sicurezza rispetto alla controparte certificata ISO 9001
- Le organizzazioni certificate **ISO/IEC 27001** hanno una **maggior predisposizione** a configurazioni di **comunicazione sicura** (50% delle aziende con valutazione A e A+)
- Le organizzazioni certificate ISO/IEC 27001 hanno una leggera prevalenza nell’aggiornare le proprie tecnologie di CMS

Prospettive dei servizi accreditati di cybersicurezza

CYBERSECURITY NATIONAL LAB

Capitolo diretto da:

Alessandro Armando

Università degli Studi di Genova
Vice Direttore Cybersecurity National Lab

Paolo Prinetto

Politecnico di Torino & IMT Scuola Alti Studi Lucca
Direttore Cybersecurity National Lab

Università di Genova

Politecnico di Torino

IMT SCUOLA ALTI STUDI LUCCA

Servizi accreditati di Cybersicurezza

- I servizi accreditati di Cybersicurezza giocano un ruolo centrale
  - nell'offrire **garanzie circa il rispetto di requisiti di sicurezza fondamentali** quali
    - la **tutela della privacy** e
    - la **protezione dell'erogazione dei servizi essenziali** dalla minaccia cyber.
  - nel **costruire relazioni di "fiducia" tra produttori e consumatori di prodotti e servizi digitali**.
- Ruolo destinato a crescere alla luce delle iniziative nazionali e comunitarie (ad es. *Strategia Nazionale di Cybersicurezza*, *Cybersecurity Act)*.

Considerazione importante

- 4.200 organizzazioni certificate da 20 CAB detentori di circa 30 accreditamenti, che, unite ai 5 Laboratori e ai Trust Service Providers in ambito SPID ed eIDAS, assommano a circa 4.300 soggetti.
- **Solo un millesimo del tessuto produttivo dell'intero Paese!**
- I Professionisti in possesso di Certificazione Professionale per gli Audit nell'ambito della sicurezza delle informazioni non superano i 40 in tutto il Paese.
- La creazione del know-how dei Professionisti impiegati non è un processo breve né semplice.

Possibili evoluzioni dei Servizi Accreditati di Cybersicurezza

- Il contesto è favorevole per un più ampio utilizzo dei servizi accreditati di Cybersicurezza, ma gli attuali schemi di certificazione non sempre soddisfano le esigenze di importanti settori del mercato.
- I tempi e i costi associati alla certificazione di prodotti e servizi spesso non sono compatibili con i vincoli finanziari e/o di *time-to-market* cui sono soggette le aziende produttrici.
- Ad esempio, non tutti i prodotti e i servizi richiedono il livello di sicurezza offerto da *ISO/IEC 15408 Common Criteria,* né le relative aziende produttrici sono in grado di sostenere i costi.
- È pertanto fondamentale che gli schemi di certificazione di Cybersicurezza possano evolvere nelle direzioni richieste dal mercato.

Schemi di Certificazione “Leggera”

- Schemi di certificazione leggera (*lightweight certification*)
  - capaci di offrire un livello di sicurezza adeguato a contesti operativi caratterizzati da un livello di rischio non elevato,
  - senza incorrere in tempi e costi particolarmente gravosi.
- Consentono di allargare significativamente la platea dei possibili fruitori con un notevole beneficio collettivo.
- Esistono iniziative nazionali (Spagna, Francia, Germania, Olanda)
- Manca però un approccio unificato.

Integrazione della Certificazione di Cybersicurezza nel Processo di Sviluppo

- **DevOps** combina le **fasi di sviluppo** (Dev) e di **messa in operazione** (Ops) del software assicurando così che le nuove funzionalità vengano messe in operazione in tempi rapidissimi e con elevato livello di qualità.
- **DevSecOps**: aspetti di sicurezza trattati in tutto il ciclo di vita dell'applicazione.
- Apre alla possibilità di inserire **controlli automatici di sicurezza** nelle varie fasi e di **generare automaticamente la documentazione necessaria per la certificazione** non solo della versione iniziale del prodotto, ma di tutte le versioni rilasciate successivamente.

Cyber Range per le Certificazioni di Cybersicurezza

I Cyber-Range offrono la possibilità di verificare la resilienza dei servizi erogati dalle aziende di fronte a minacce sofisticate e pervasive (ad es. ransomware).

I Cyber-Range

- offrono un'**inedita opportunità per la creazione di schemi di certificazione di nuova generazione**,
- basati sulla **verifica dell'efficacia delle misure di sicurezza e della resilienza dei sistemi in condizioni molto simili a quelle di esercizio** e
- con **sollecitazioni corrispondenti ad attacchi sofisticati e di larga scala**.
- Bacino d'utenza potenziale molto ampio, che include il settore finanziario, delle telecomunicazioni, energetico e dei trasporti.

Certificazioni di cybersecurity per le PMI

- Sia gli schemi di certificazione sia i framework di cybersecurity sono spesso realizzati avendo come obiettivo primario le grandi organizzazioni.
- Complessità e costi sono spesso fuori dalla portata delle aziende meno strutturate e con limitate capacità di spesa, quali ad esempio le PMI.
- Questo è un problema acuto, specialmente per il nostro Paese, la cui economia è caratterizzata da una presenza molto consistente di PMI.
- Secondo ECSO la quasi totalità (98%) delle 60.000 aziende che operano nel mercato europeo della Cybersecurity sono PMI o Start-up.
- Pur esistendo soluzioni offerte nei vari paesi europei, manca uno schema di certificazione unificato dedicato alle PMI.

Considerazioni Finali

Certificazione e Accreditamento: i Casi di Studio

- I casi di studio hanno evidenziato un significativo grado di maturità del campione selezionato circa la consapevolezza del rischio informatico e i benefici apportati dal processo di certificazione ISO 27001.
- L'acquisizione della consapevolezza richiede tempo, perché identificare gli elementi che permettono di percepire i benefici non è immediato, ma anche perché essi derivano da dinamiche complesse, messe in luce dallo studio.
- La ISO 27001 è elemento trainante per la postura dell'organizzazione rispetto al tema della conformità a norme, standard e regolamenti.
- Le strategie utilizzate per l'adozione dello standard sono diversificate in funzione delle caratteristiche dell'organizzazione (dimensione e diversificazione delle funzioni).

Certificazione e Accreditamento: l'Attività sul Campo

- Pur non essendo una valutazione di sicurezza esaustiva, l'attività di *vulnerability assessment* fornisce **indizi** molto chiari circa la postura di sicurezza dell'organizzazione considerata.
- I servizi web sono infatti quelli maggiormente sfruttati dagli attaccanti per assicurarsi il punto di ingresso nel perimetro dell'organizzazione.
- Il risultato, che mostra una chiara correlazione tra la **minore suscettibilità ad attacchi web delle organizzazioni certificate ISO 27001 rispetto a quelle certificate ISO 9001**, non è irrilevante.
- Mostra che anche in un dominio caratterizzato da elevata attenzione verso la qualità di processo (ISO 9001), non si sviluppano una sufficiente attenzione verso la Cybersicurezza e adeguate capacità di gestione della stessa, se non si affronta un processo di certificazione specifico (ISO 27001).

Prospettive dei Servizi Accreditati di Cybersicurezza

- Il contesto è favorevole per un più ampio utilizzo dei servizi accreditati di Cybersicurezza, ma gli attuali schemi di certificazione non sempre soddisfano le esigenze di importanti settori del mercato.
- È pertanto fondamentale che gli schemi di certificazione di Cybersicurezza possano evolvere nelle direzioni richieste dal mercato:
  - Certificazione Leggera
  - Cyber Range per le Certificazioni di Cybersicurezza
  - Integrazione della Certificazione di Cybersicurezza nel Processo di Sviluppo
  - Certificazioni di Cybersicurezza per le PMI

Il Gruppo di Lavoro

ACCREDIA

- Riccardo Bianconi
- Amerigo Cancellieri
- Gianluca Di Giulio
- Lorenza Guglielmi
- Alessandro Nisi
- Guglielmo Tozzi
- Pietro Vitaliano
- Alessandra Zacchetti

Cybersecurity National Lab

- Alessandro Armando
- Francesco Buccafurri
- Fabio De Rosa
- Giorgio Giacinto
- Paolo Prinetto
- Leonardo Querzoni
- Luca Verderame

In collaborazione con:

CYBERSECURITY NATIONAL LAB

ACCREDIA

L'ENTE ITALIANO DI ACCREDITAMENTO

Grazie per aver partecipato!