Il CERT della Pubblica Amministrazione

Ruolo, funzione e servizi erogati

Corrado Giustozzi
Agenzia per l'Italia Digitale – CERT-PA

Formez, 11 dicembre 2018

Premessa

COS’È ESATTAMENTE UN CERT?

Il primo incidente in Rete…

- Alle 18:00 del 2 novembre 1988 Robert Tappan Morris, dottorando in informatica della Cornell University, rilascia su ARPAnet un software capace di replicarsi sfruttando alcune vulnerabilità dei sistemi Unix
  - Tappan è figlio di Robert Morris sr., già ricercatore ai Bell Labs, dove aveva sviluppato Multics e Unix, e chief scientist alla NSA
- Il worm doveva essere solo un esperimento per testare le vulnerabilità della rete, ma sfugge di mano al suo autore e si diffonde rapidamente saturando la rete
  - vengono bloccate circa 6.000 macchine, il 10% del totale
- Morris verrà condannato a tre anni di libertà vigilata, 400 ore di servizi sociali e 10.500 dollari di multa
  - oggi insegna al Lab for Computer Science del MIT

…e la prima risposta coordinata

- Cessata l'emergenza l'agenzia DARPA, che sovraintendeva alla gestione di ARPAnet, decise di creare un programma di preparazione e risposta sistematica agli incidenti informatici
- Nel novembre 1988 venne così costituito il primo **Computer Emergency Response Team** a Pittsburgh, presso il Software Engineering Institute (SEI) della Carnegie-Mellon University
- Il termine CERT venne quindi utilizzato informalmente da altre organizzazioni simili, nate in seguito nel mondo
  - l'opposizione della CMU, che detiene i diritti sul termine CERT, portò in seguito al conio del termine CSIRT
- Oggi il SRI-CMU ospita il CERT/CC, ossia il centro di coordinamento dei principali CERT mondiali

CERT

Software Engineering Institute
Carnegie Mellon University.

La terminologia è importante

- Oggigiorno i termini CERT e CSIRT sono usati in modo piuttosto intercambiabile, ma in origine le sigle avevano significati specifici che caratterizzavano in modo preciso il tipo di organizzazione e di servizi resi alla constituency
  - tuttavia la CMU sostiene ora che CERT non è (più) un acronimo!
- CERT:
  - **Computer** Emergency **Response** Team
  - **Computer** Emergency **Readiness** Team
  - **Cyber** Emergency **Response** Team
  - **Cyber** Emergency **Readiness** team
- CSIRT:
  - **Computer** Security Incident Response Team
  - **Cyber** Security Incident Response Team

Servizi standard di un CERT

Reactive Services	Proactive Services	Security Quality Management Services

• **Alerts and Warnings**
• **Incident Handling**
  • **Incident analysis**
  • Incident response on site
  • **Incident response support**
  • **Incident response coordination**
• Vulnerability Handling
  • Vulnerability analysis
  • Vulnerability response
  • Vulnerability response coordination
• Artifact Handling
  • Artifact analysis
  • Artifact response
  • Artifact response coordination
	• **Announcements**
	• Technology Watch
	• Security Audits or Assessments
	• Configuration and Maintenance of Security Tools, Applications, and Infrastructures
	• Development of Security Tools
	• Intrusion Detection Services
	• Security-Related Information Dissemination
		• Risk Analysis
		• Business Continuity and Disaster Recovery Planning
		• Security Consulting
		• Awareness Building
		• Education/Training
		• Product Evaluation or Certification

Fonte: ENISA e CERT/CC

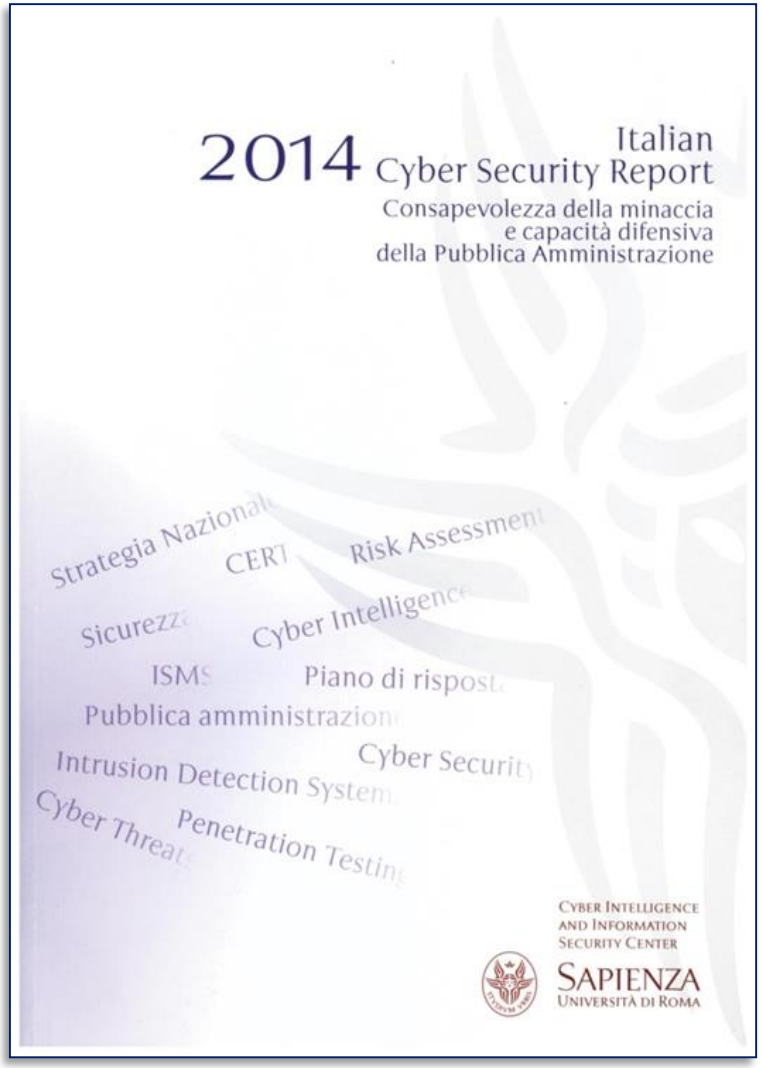
I “clienti” del CERT

- La **constituency**:
  - è la *comunità di riferimento*, ossia l’insieme di clienti, interni o esterni all’organizzazione cui il CERT appartiene, verso cui il CERT eroga istituzionalmente i propri servizi
- Le eventuali **community**:
  - il CERT può intrattenere rapporti con ulteriori entità non comprese nella propria constituency, le quali possono essere organizzate all’interno di una o più *community* formali
  - le principali interazioni con le community consistono solitamente in *scambi informativi* strutturati, dei quali beneficiano mutuamente tutte le parti in gioco
  - la partecipazione ad una community può essere regolata da specifici accordi bilaterali (MoU, protocolli d’intesa) o da un regolamento generale della community stessa
- Eventualmente anche il pubblico generale

La struttura a servizio della PA

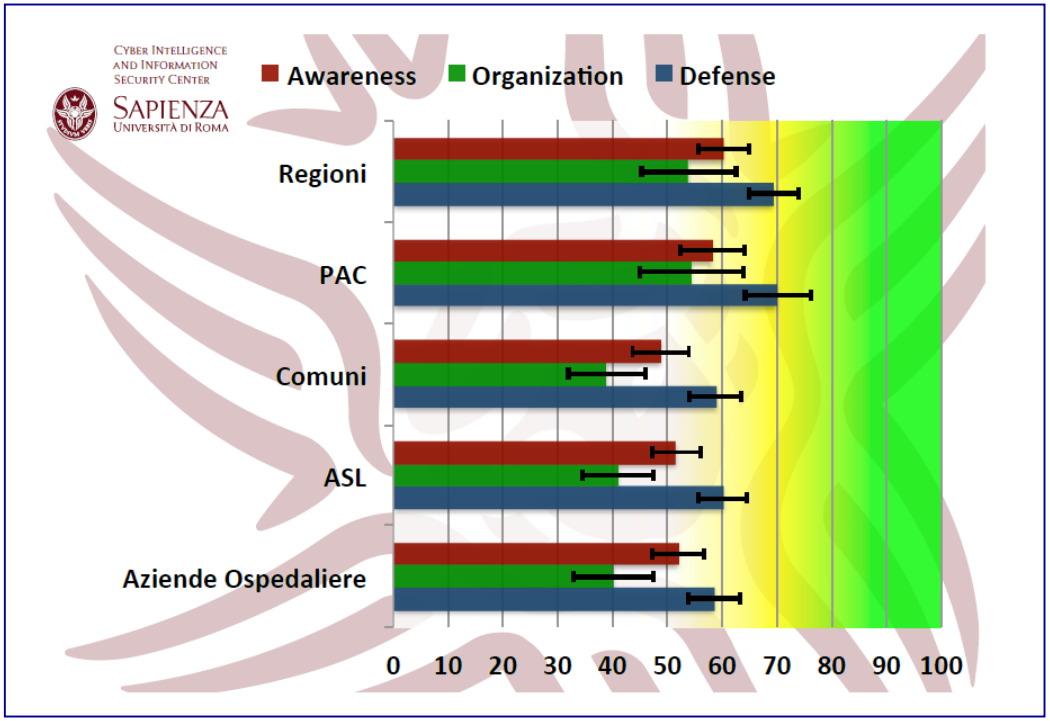
IL CERT DELLA PUBBLICA AMMINISTRAZIONE

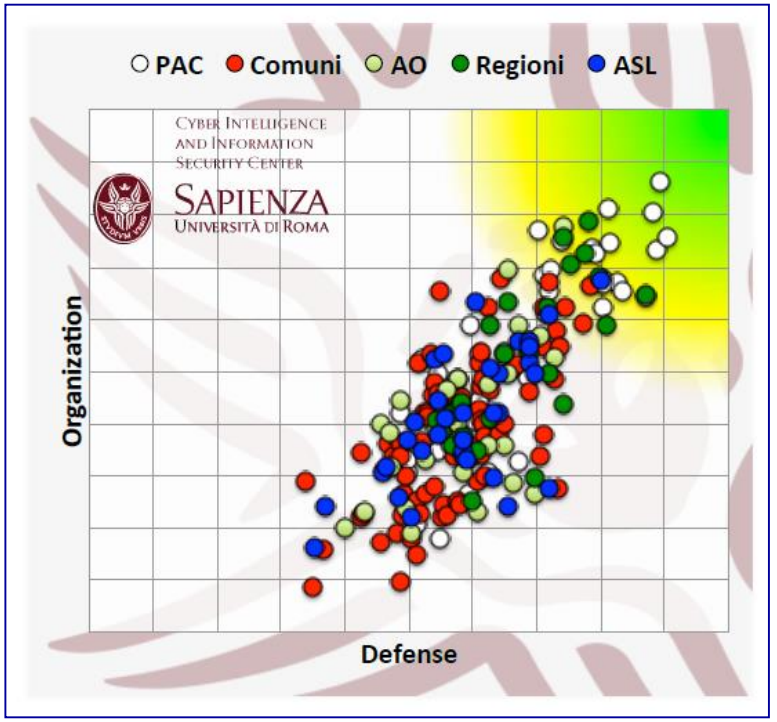
I razionali: la situazione nella PA



- Sicurezza basata sulle tecnologie
- Mancanza di strutture organizzative in grado di gestire gli eventi e rispondere agli attacchi
- Superficie d'attacco eccessiva
- Mancanza di una *baseline* comune di riferimento

Una Pubblica Amministrazione vulnerabile

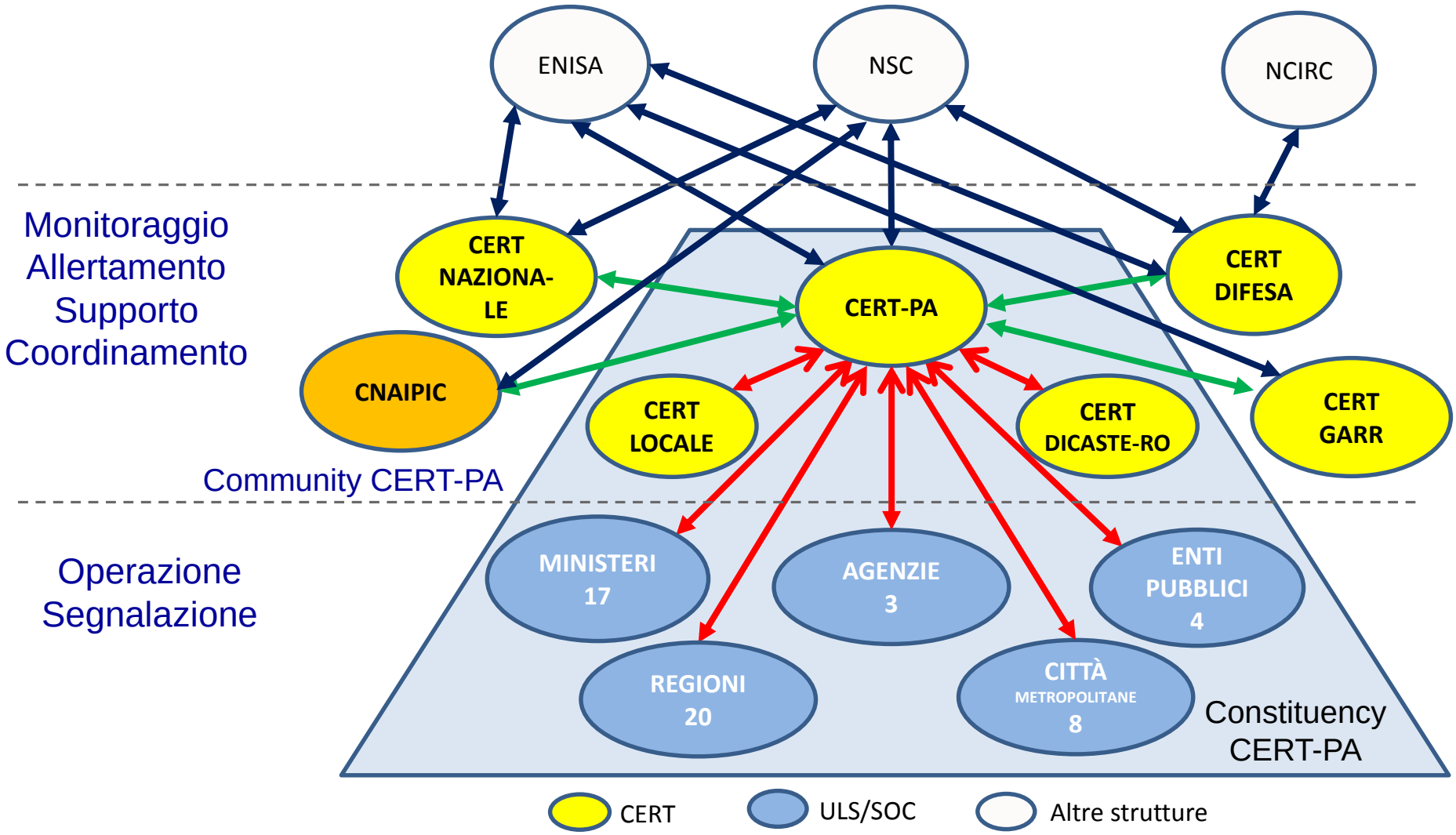




Il ruolo di AgID nel QSN

- Regole tecniche e linee guida
- Protezione patrimonio informativo
- Razionalizzazione dei CED
- Servizi erogati dalle PA
- Formazione
- CERT-PA

Il ruolo del CERT-PA (pre 2017)



Il CERT-PA in breve

- Creato nel 2013 (sulla base dell'esperienza del precedente CERT-SPC), a regime dal 2015
- Opera all'interno dell'Agenzia per l'Italia Digitale:
  - inserito nei principali circuiti di CERT internazionali
  - componente dell'Architettura Nazionale per la protezione dello spazio cibernetico
- Constituency:
  - iniziale: Pubbliche Amministrazioni Centrali, Regioni, Città Metropolitane (~70 Amministrazioni)
  - *de facto*: ~22.000 Amministrazioni (modalità *best effort*)
- Monitoraggio continuo dell'intero spazio di domini *.gov.it
- Fornisce servizi proattivi e reattivi alle Amministrazioni accreditate
- Fornisce supporto agli incidenti laddove richiesto

Accreditamenti internazionali

- Registrato nell'indice degli CSIRT europei mantenuto da ENISA

- Accreditato da Trusted Introducer

- Riconosciuto dal CERT/CC (CMU), autorizzato ad usare il nome CERT

I servizi erogati dal CERT-PA

Reactive Services	Proactive Services	Security Quality Management Services

• **Alerts and Warnings**
• **Incident Handling**
  • **Incident analysis**
  • Incident response on site
  • **Incident response support**
  • **Incident response coordination**
• Vulnerability Handling
  • Vulnerability analysis
  • Vulnerability response
  • Vulnerability response coordination
• Artifact Handling
  • Artifact analysis
  • Artifact response
  • Artifact response coordination
	• **Announcements**
	• Technology Watch
	• Security Audits or Assessments
	• Configuration and Maintenance of Security Tools, Applications, and Infrastructures
	• Development of Security Tools
	• Intrusion Detection Services
	• Security-Related Information Dissemination
		• Risk Analysis
		• Business Continuity and Disaster Recovery Planning
		• Security Consulting
		• Awareness Building
		• Education/Training
		• Product Evaluation or Certification

Fonte: ENISA e CERT/CC

Threat intelligence e analisi della minaccia

- Analisi svolte autonomamente su fonti qualificate aperte e semiaperte (nessuna informazione acquisita da fonti commerciali e/o a pagamento):
  - gestite ~2.500 segnalazioni
  - acquisiti ed elaborati ~7.000.000 IoC
- Attività di verifica, validazione degli IoC, trasformazione in IoC qualificati e loro pubblicazione:
  - emessi ~37.300 IoC qualificati (~12.600 IP, ~24.600 URL)
  - analizzati ~17.700 malware
- Trasmissione automatizzata ad un primo gruppo sperimentale di soggetti qualificati (~15) mediante piattaforma integrata con i tool del CERT-PA, basata su protocolli standard (STIX-TAXII) e piattaforme open (sviluppo a cura del CERT-PA)

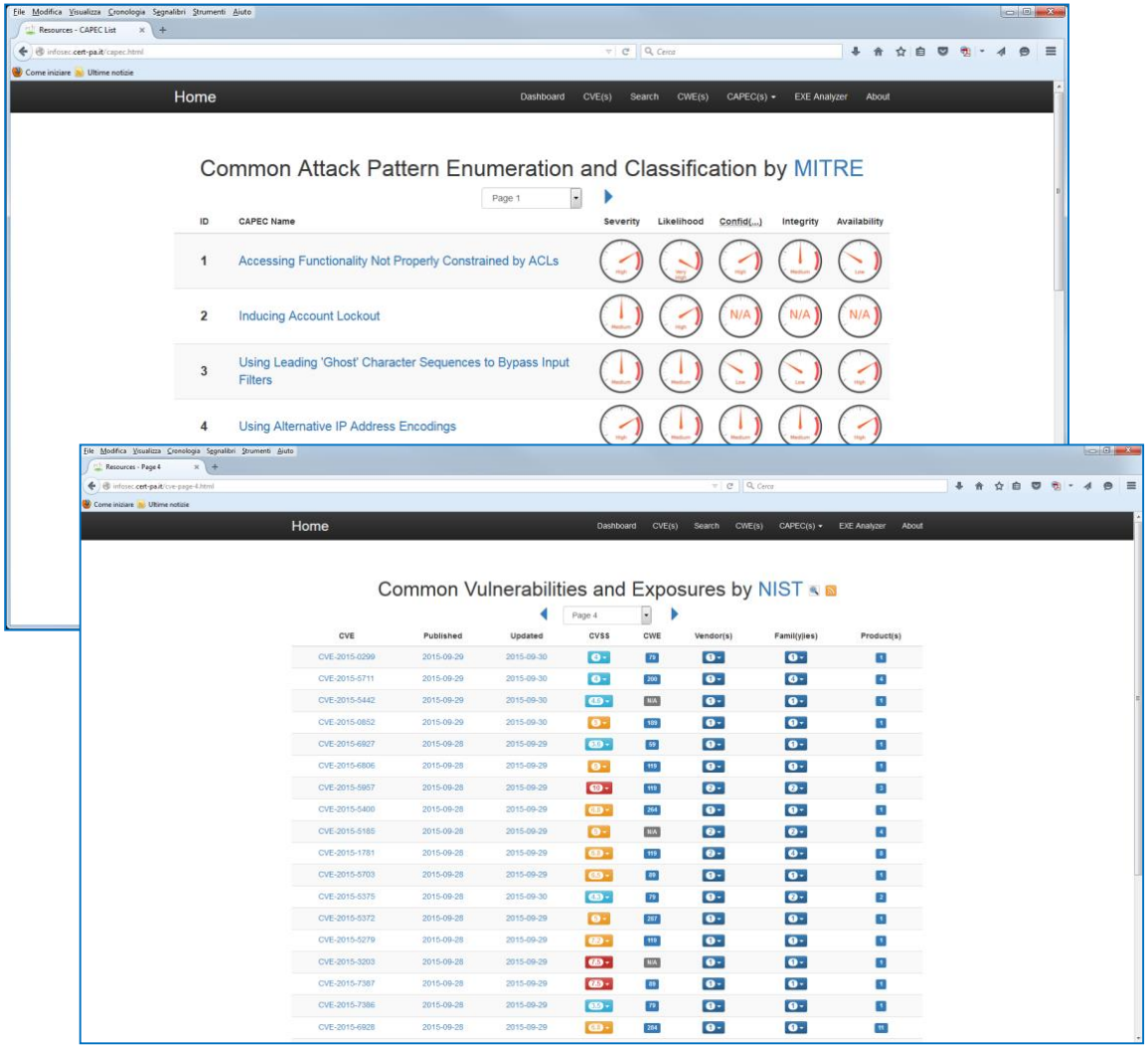
Infosharing

- Scambio continuo di informazioni «actionable» (ossia: immediatamente utilizzabili in ambito operativo) su:
  - minacce e agenti di minaccia
  - campagne in corso
  - vulnerabilità
  - exploit
  - indicatori di compromissione (IoC)
- Le informazioni analizzate provengono sia dalle attività di monitoraggio e analisi svolte direttamente dal CERT-PA, sia da scambi informativi con soggetti qualificati della Community

Modalità di accreditamento e benefici

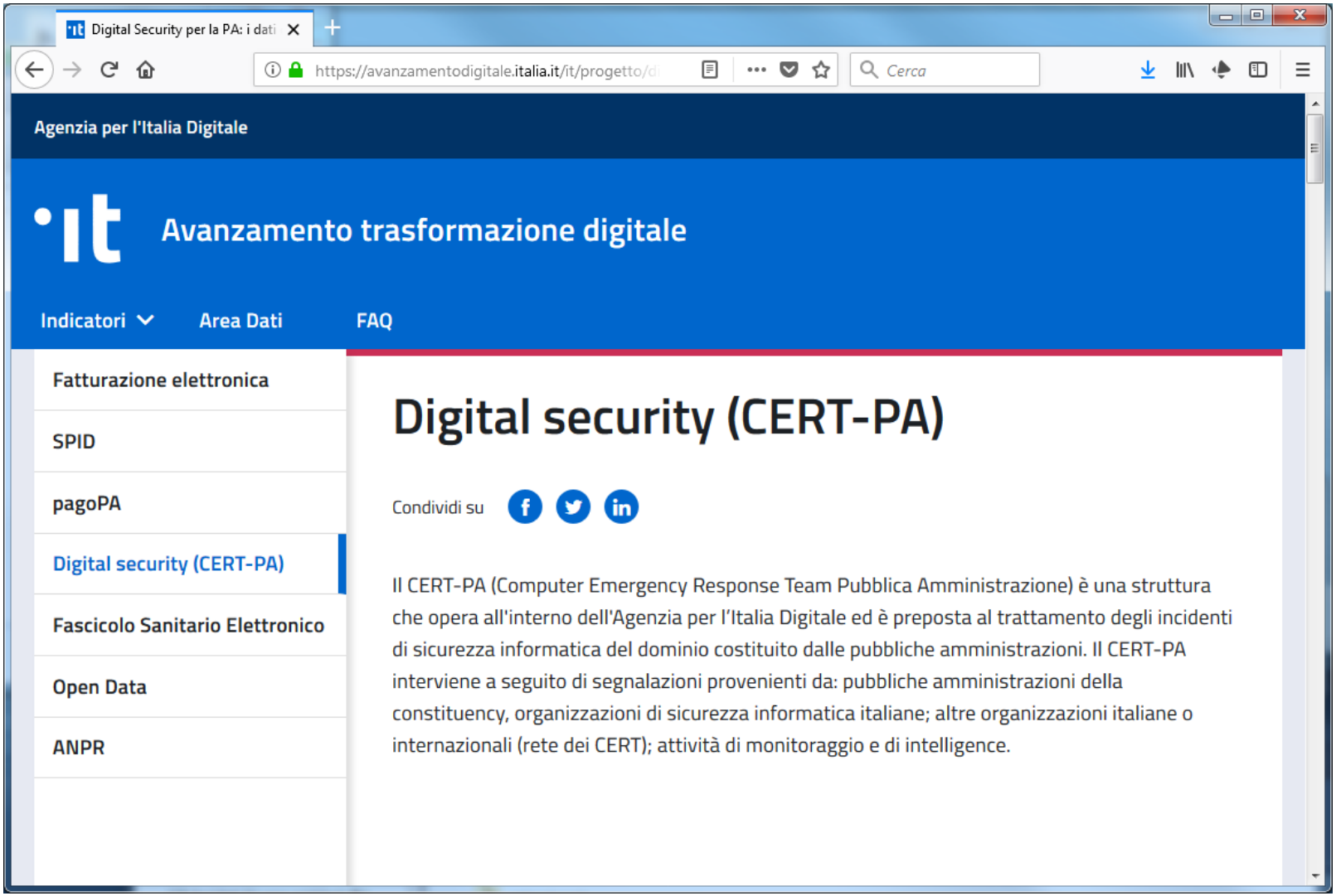
- Le Amministrazioni attualmente accreditabili sono:
  - quelle della *constituency* originaria (PAC, Regioni, Città metropolitane)
  - le loro società *in-house* di informatica, su richiesta dell'Amministrazione
- Processo di accreditamento:
  - l'Amministrazione richiede l'accreditamento via semplice e-mail
  - il CERT-PA invia al responsabile un modulo anagrafico da compilare
  - l'Amministrazione invia al CERT-PA le informazioni richieste
- L'informazione cruciale è quella relativa al referente (o più d'uno) che avrà il ruolo di interfaccia verso il CERT-PA
- L'Amministrazione accreditata usufruirà di:
  - un account ed un'area riservata sulla piattaforma di servizi del CERT-PA
  - l'attivazione del monitoraggio continuo sul proprio dominio
  - la ricezione tempestiva di alert e bollettini non pubblici
  - l'eventuale ricezione di comunicazioni specifiche
  - il supporto degli specialisti del CERT-PA a seguito di eventuali incidenti

Tool a disposizione di tutti: infosec



- Elemento centrale per il National Italian Vulnerability Database
- Console interattiva Web-based
- Fornisce statistiche e dati analitici su Pattern di attacco, Vulnerabilità e IoC (Indicatori di compromissione)
- Disponibile a tutti (in consultazione) su infosec.cert-pa.it

Le statistiche disponibili on-line



AGID | Agenzia per l'Italia Digitale

Il Paese che cambia passa da qui.

agid.gov.it

corrado.giustozzi@agid.gov.it

@cgiustozzi