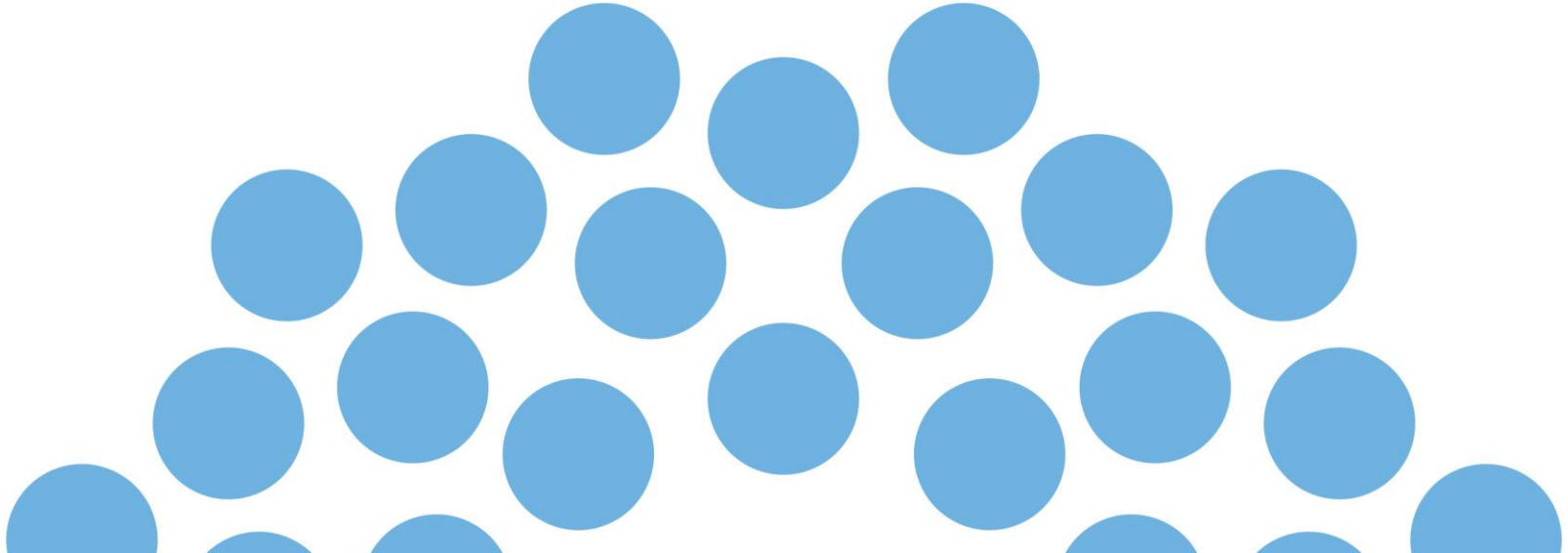
InfoCamere: Sicurezza degli asset digitali delle CCIAA italiane

Enrico Notariale
14/12/2017



Asset digitali e valore dell'informazione (1/2)

Una nuova ecumene

Viviamo in un momento di profonda trasformazione: il nostro spazio abitato si espande dai confini geografici verso un nuovo mondo.

La dimensione digitale

Asset digitali e valore dell'informazione

Nel mondo digitale ritroviamo

IDENTITA'

BENI

LUOGHI

Per esempio.. InfoCamere

E’ il luogo dove risiedono le informazioni del sistema camerale

Per esempio.. InfoCamere

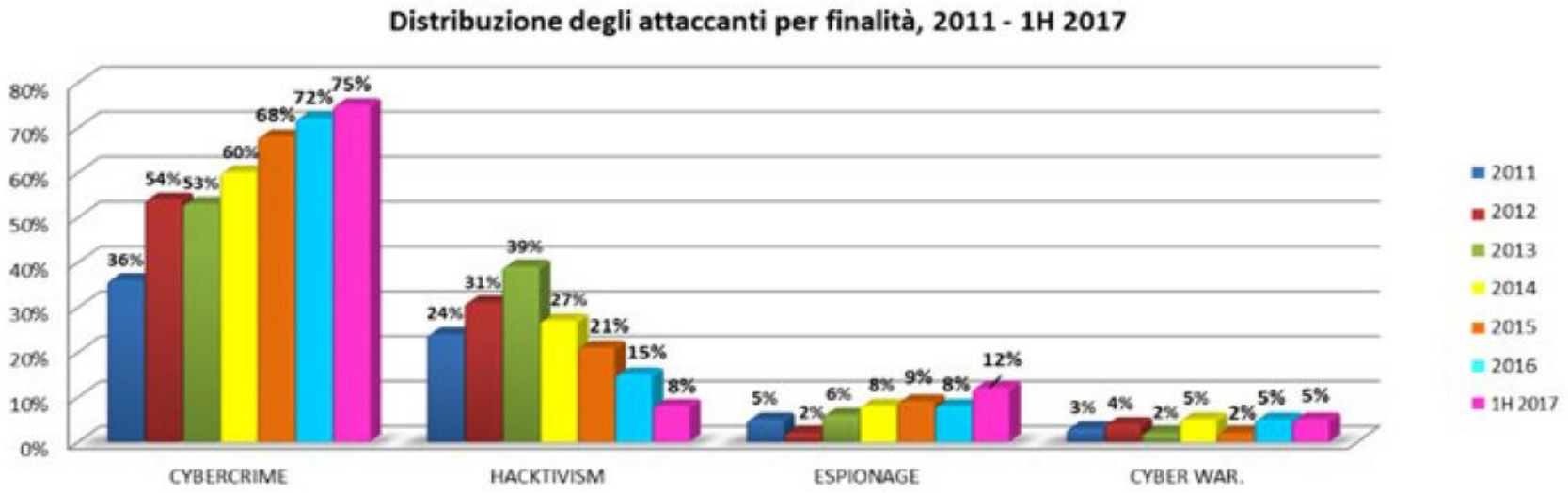
La casa dei dati del sistema camerale

VIDEO DATA CENTER INFOCAMERE

Minacce

L’industria del Cybercrime

Panoramica dei cyber attacchi più significativi del 2016 e del primo semestre 2017

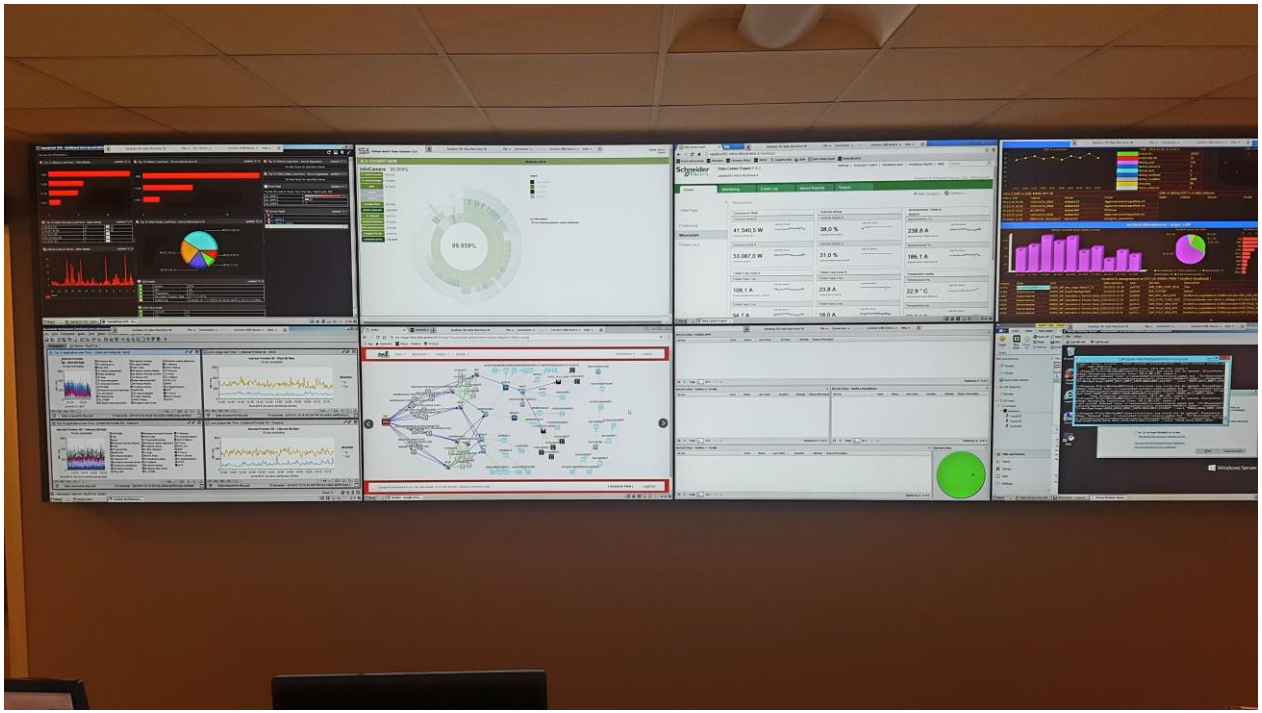


© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia - aggiornamento giugno 2017

Per esempio.. InfoCamere

Il cybercrime opera di continuo e da ogni dove

I tentativi di attacco sono continui e vanno opportunamente bloccati grazie a strumentazioni tecniche adeguate ed aggiornate



Le sorgenti degli attaccanti sono le più disparate

Per esempio.. InfoCamere

Organizzazione

Sistema di gestione della sicurezza delle informazioni (ISO27001:2013)

- commitment della direzione
- controlli e miglioramenti **continui**
- **ruoli** e responsabilità di sicurezza nei processi
- **policy**
  - **politiche di sicurezza** con i principi generali: separazione dei compiti per attività delicate, need to access, …
  - procedure, istruzioni tecniche e manuali operativi

Analisi dei **rischi**:

- Business Impact Analysis,
- piani di trattamento del rischio

Controlli su più livelli:

- controlli e report di sicurezza
- visita di Certificazione esterna ISO27001:2013
- verifiche di internal auditing

Per esempio.. InfoCamere

Processi in InfoCamere

Risorse Umane:

- selezione, formazione, responsabilizzazione delle persone
- regole generali chiare per tutti i dipendenti: password, gestione stazioni di lavoro, riservatezza dei documenti, …

Sicurezza e privacy fin dalla progettazione, **by design & by default:**

- realizzazione ed evoluzione dei servizi informatici
  - architetture, crittografia comunicazioni/dati, data masking, etc..
- approvvigionamenti (requisiti contrattuali con i fornitori)

Gestione accessi logici

Identity management e Access management (single sign on) che permette l'uso di differenti tipologie di credenziali: user e psw, SPID, CNS, OTP

- gestione credenziali e abilitazioni
  - provisioning, gestione, controlli, rimozione
- controllo accessi
- controlli abilitazioni periodici

Per esempio.. InfoCamere

Strumenti in InfoCamere

Reti di comunicazione tra i data center e centinaia di sedi del sistema

- reti dedicate e ridondate (su fornitori diversi)
- amministrate internamente centralmente
- reti con protezioni e controlli differenziati
- separazione degli ambienti di produzione, sviluppo, test
- strumenti: firewall, IPS e altri strumenti di controllo del traffico

Alta affidabilità: sistemi, reti, alimentazione, …

Disaster Recovery presso il data center di Milano

Sicurezza **fisica**

- protezione perimetrale: videosorveglianza, allarmi, vigilanza
- controlli degli accessi fisici a più livelli con più strumenti (badge, pin)
- protezione del sito da eventi naturali, energetici, etc.: batterie, generatori e serbatoi,
- sicurezza fisica dei lavoratori nelle emergenze!

Per esempio.. InfoCamere

Integrazione tra processi e strumenti in InfoCamere

Gestione sicura degli **asset**

- acquisto
- manutenzione/aggiornamento
- … fino alla dismissione!

Protezione dei sistemi

- **antimalware**, antivirus, antispam
- **hardening** dei sistemi
- **patch** management (stazioni di lavoro, ambienti di produzione)

Processi di **Backup**

- totali, incrementali …
- stazioni di lavoro virtuali

Gestione dei **log**

- sistemistici, applicativi, accounting, accessi, …
- Security Information and Event Management - SIEM

Per esempio.. InfoCamere

Controlli in InfoCamere

Security Operation Center

- Esterno (minacce, alert e eventi di sicurezza)
- Interno (eventi di sicurezza, remediation e mitigazione)

Processi (e strumenti) di **controllo:**

- **Change** management
- **Event** management,
- **Incident** management,
- **Problem** management

Verifica (interna ed esterna) delle **vulnerabilità**:

- VA/PT applicazioni
- VA/PT sistemi ed infrastrutture

Consulenza interna ed esterna:

- Specialisti di sicurezza e compliance (processi e controlli)
- Specialisti di protezione (tecnici informatici)

Sicurezza delle informazioni

Riflessioni finali

La sicurezza delle informazioni:

- necessita di **un'attività continua** di analisi, riesame e miglioramento
- deve seguire la vita dell'organizzazione
- deve essere 'cucita su misura' sulle proprie esigenze specifiche.

Ciò può essere fatto solo raccogliendo **input a 360°:**

- analisi dei rischi
- indicazioni di audit e/o assessment (interni ed esterni)
- segnalazione e raccolta degli eventi
- gestione incidenti e problemi interni, notizie di incidenti esterni
- strumenti e processi di controllo
- analisi di nuovi servizi e nuovi approvvigionamenti
- aggiornamento continuo sull'evoluzioni di norme, standard, best practice
- attenzione alle proposte del mercato (consulenze, segnalazioni, suggerimenti, strumenti)
- indicazioni di soggetti si occupano di analisi, reporting, andamenti in ambito sicurezza

IC
InfoCamere
Innovare è Crescere

Grazie per l’attenzione.

twitter.com/infocamere
infocamere.it