CSA
Cyber Security @ngels
Academy

Gli elementi “difficili” per gestire la sicurezza delle informazioni

24 gennaio 2023 – Cesare Gallotti

Le misure di sicurezza

Le conosciamo già. Possiamo riprenderle dalla ISO/IEC 27002:

- Governo (regole e procedure)
- Gestione degli asset
- Classificazione e trattamento delle informazioni
- Gestione del personale
- Sicurezza fisica
- Sicurezza dei sistemi e delle reti
- Sicurezza applicative
- Configurazioni sicure
- Gestione delle identità e degli accessi
- Gestione delle minacce e delle vulnerabilità
- Continuità
- Relazioni con i fornitori
- Conformità contrattuale, regolamentare e legale
- Gestione degli eventi di sicurezza delle informazioni
- Garanzia della sicurezza delle informazioni

Però...

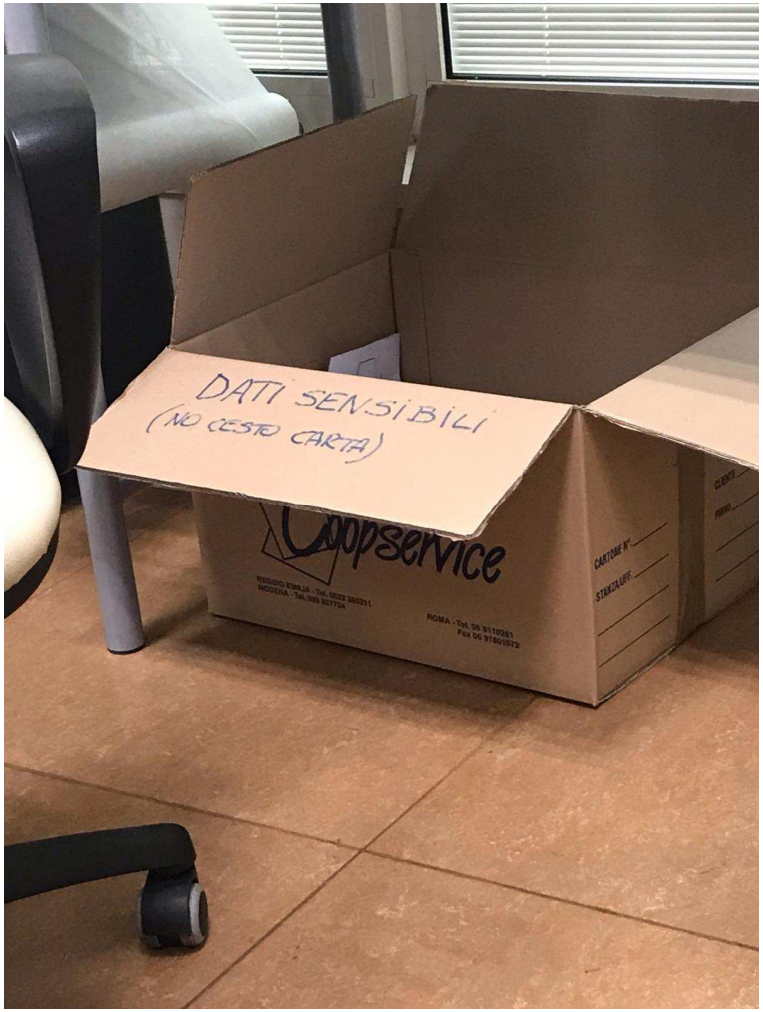
Però alcune sono più difficili di altre da realizzare per:

- costo;
- difficoltà tecniche;
- difficoltà organizzative.

L’asset inventory

- Asset diversi richiedono inventari diversi, ma non tutti lo capiscono.
- Per alcuni è più facile ricordarli che scriverli.
- Nelle realtà complesse sono necessari strumenti di discovery.

Etichettare le informazioni



Controllo dei dispositivi

- Si fa accedere a email e file con dispositivi personali, senza alcun controllo (cifratura, patching, antivirus, attivazione del controllo accessi).
- In molti casi, anche i dispositivi aziendali (smartphone e tablet) non sono gestiti.
- Con i pc (fissi e portatili) la situazione è migliore.
- Paura per la privacy? Cultura per cui il dispositivo si usa come si vuole?

Aggiornare i sistemi

Lo sappiamo:

- se aggiorniamo troppo presto, rischiamo il blocco;
- se aggiorniamo troppo tardi, rischiamo di essere attaccati.

Molti non hanno però alcun sistema di controllo centralizzato.

Sistema di logging

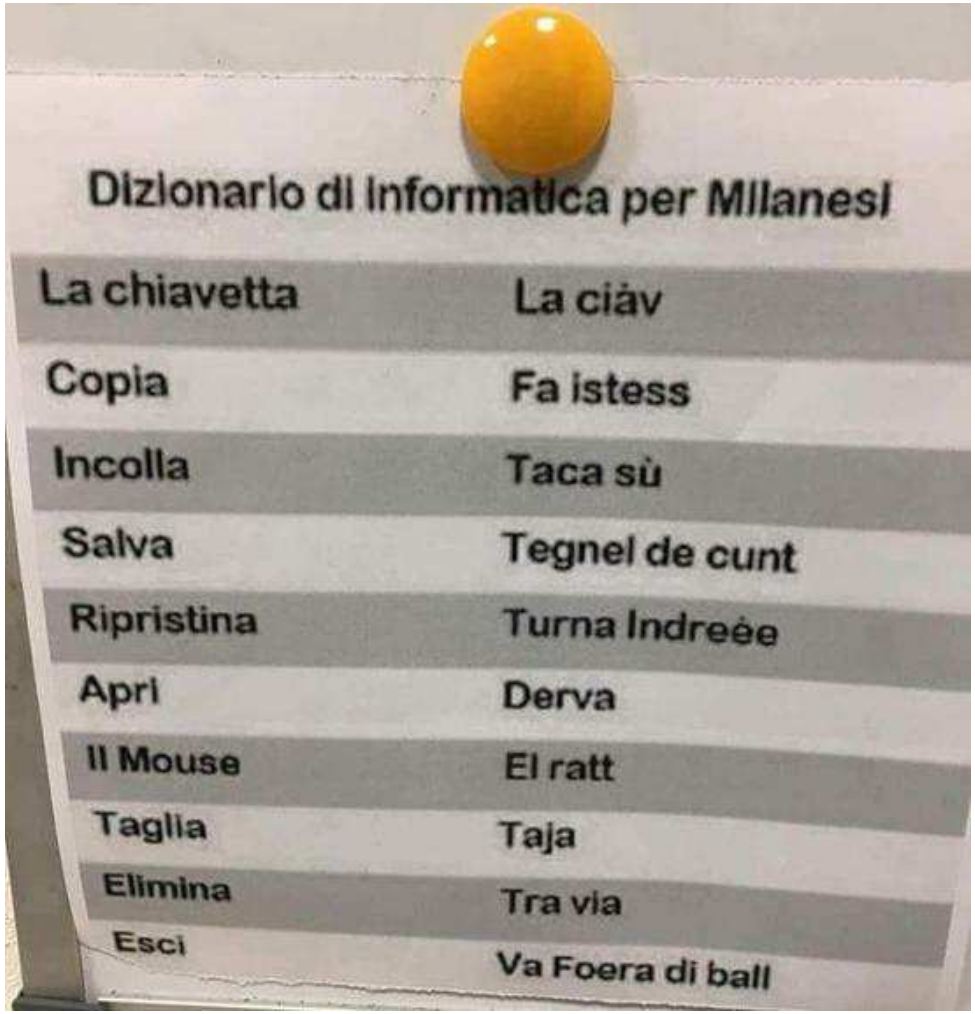
- Centralizzato
- Che permette analisi
- Che lancia allarmi

Threat intelligence

- Quali canali seguire?
- Solo i bollettini dei produttori di software?

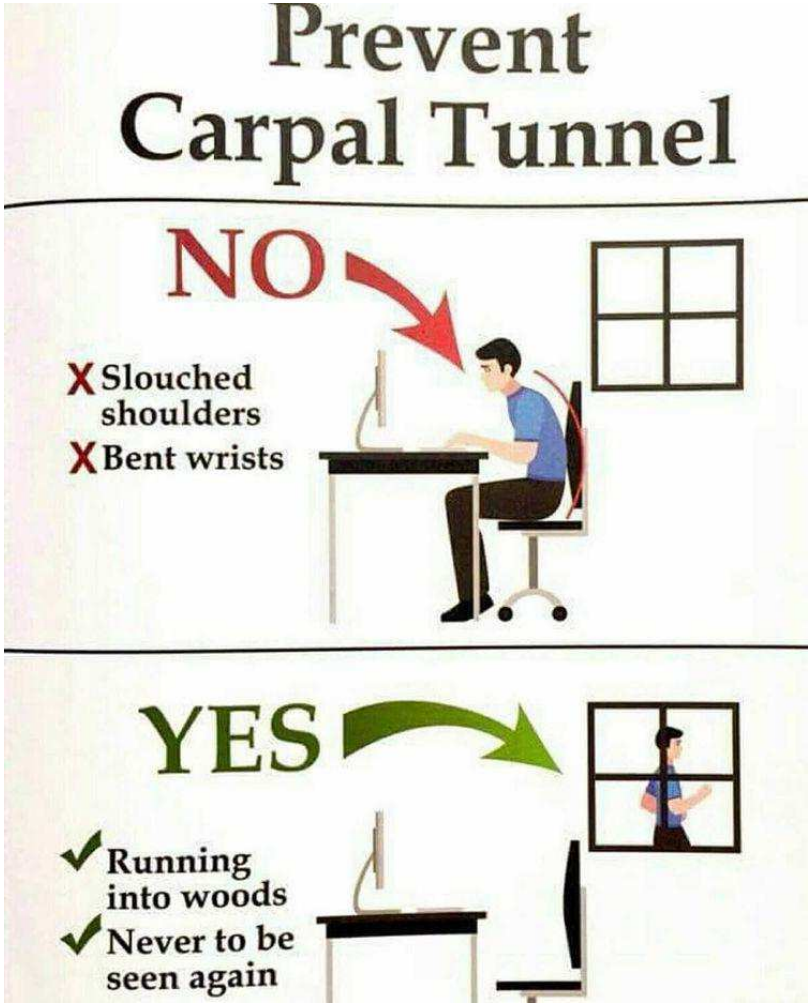
Corsi tecnici

- Sono fatti corsi «trasversali» (inglese, gestire il tempo, migliorare i rapporti con i clienti, team building).
- Ma i corsi tecnici sono rari.
- Molta auto-formazione, che ha i suoi limiti.



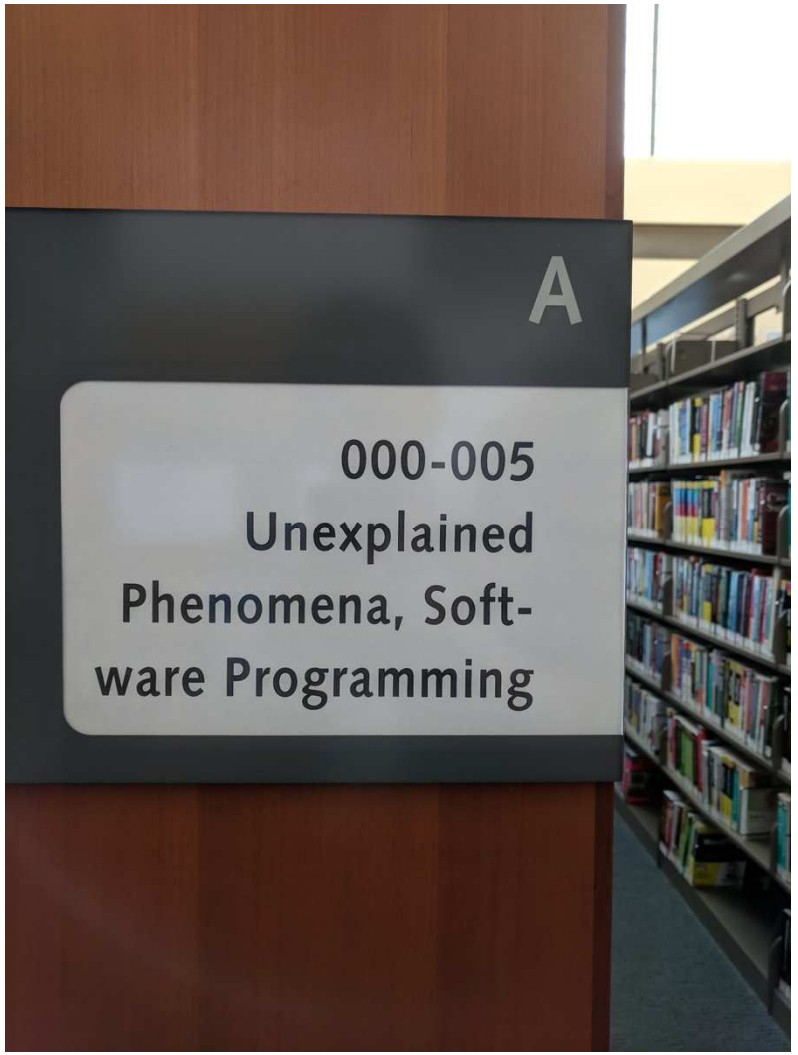
Associazioni

- Confrontarsi con altri è fondamentale.
- Quali associazioni? In effetti non ce ne sono molte...



Processo di sviluppo sicuro

- Non si documentano i requisiti di sicurezza.
- Non si pianifica (neanche i test).
- Non si documentano (sperando che si facciano...) i test funzionali e di sicurezza.
- Forse le competenze non sono così complete?



Tracciare i change e gli eventi

Difficile è anche categorizzare le segnalazioni per avere report.

Sembra però sempre più facile fare che fare e tracciare.

CSA
Cyber Security @ngels

Dobbiamo “inventarci” una sorta di “anormale normalità”. Dobbiamo continuare a tenerci in contatto, interagire, comunicare in seno alle communities e verso l’esterno.