Convegno: «Equità e sostenibilità: una necessaria trasformazione antropocentrica dell'impresa»

Prevenzione del data breach: suggerimenti per le PMI

a cura di:

Prof. Cataldo Basile

Torino, 18 novembre 2022

Data breach e non solo…

- il data breach è solo uno degli incidenti informatici che possono avvenire in una PMI
  - furto di proprietà intellettuale
  - attacchi alle email
  - compromissione di sistemi e di linee di produzione
  - DDoS: negazione di un servizio
  - attacchi alle supply chain

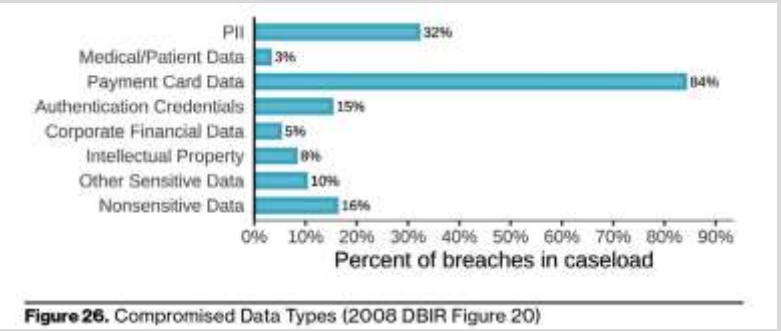


Figure 26. Compromised Data Types (2008 DBIR Figure 20)

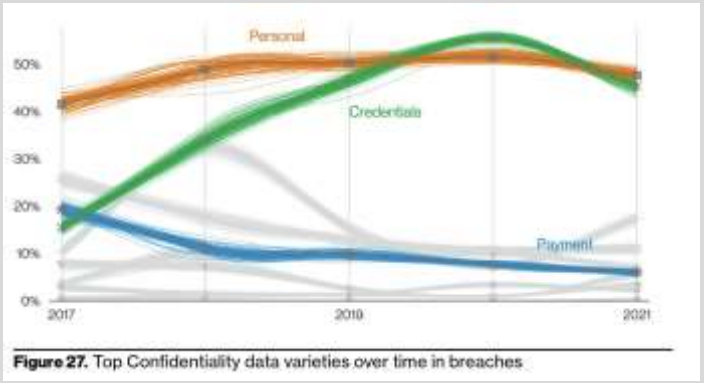
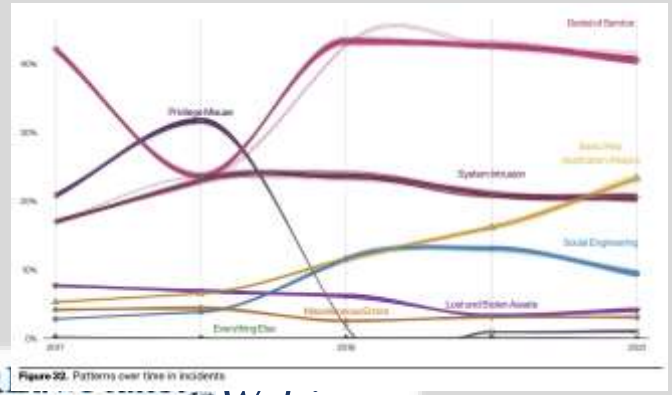


Figure 27. Top Confidentiality data varieties over time in breaches



https://www.verizon.com/business/resources/reports/dbir/
(cfr. pagg. 75-76)

"La sicurezza è un processo, non un prodotto"

- ...Bruce Schneier... nel 2000
  - https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html
- sviluppare una mentalità per la cybersecurity che si acquisisce col tempo e con la pratica
  - gestione del rischio informatico
- non fidarsi delle soluzioni commerciali che dichiarano di risolvere (completamente) il problema
- non affidare la gestione sicurezza a terze parti
  - anche se in alcuni casi può aiutare

Cataldo Basile
cataldo.basile@polito.it

Puntare sull'analisi dei rischi

- basata su diverse fasi valutazione di
  - identificazione di asset
  - valutazione minacce
  - scelta delle mitigazioni
  - monitoring
- esempi
  - NIST SP 800-39, SP 800-37 Rev. 2, SP 800-53 Rev. 5
  - ENISA RM/RA Framework
  - ...ma anche GDPR, ISO 21434 (TARA), ISO 27k

NIST

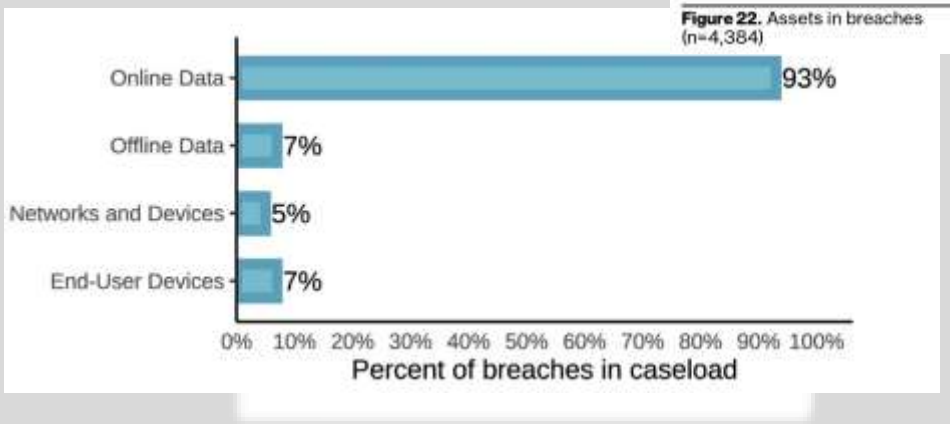
enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

Cataldo Basile
cataldo.basile@polito.it

"Conosci te stesso"

- non c'è possibilità di protezione se non si conosce cosa proteggere
  - quali sono i dati relativi alla privacy, quali i segreti industriali/progetti, etc.
    - chi può acedere? Come sono protetti? …
  - quali server/servizi sono raggiungibili e da parte di chi?
  - dove sono i dati? (es. in cloud?)
  - metodologia proposta dall'ENISA
    - https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis
- …e se non si conosce chi è il nemico
  - threat landscape ENISA
    - https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis

Figure 22. Assets in breaches (n=4,384)



Cataldo Basile
cataldo.basile@polito.it

Il management aziendale deve partecipare alla cybersecurity

- cybersecurity spesso derubricata a normale attività IT
- se ne occupano uno o più dipendenti "tecnici"
  - conservano credenziali, memoria storica, conoscenza dei sistemi
  - ...senza documentazione di riferimento o policy
  - prendono decisioni che possono avere effetto sul business e anche sul valore dell'azienda
- a breve questo avrà impatto su finanziamenti, investimenti
  - e costo assicurazioni

Cataldo Basile
cataldo.basile@polito.it

Investire in formazione

- innanzitutto per il personale coinvolto nelle attività di cybersecurity
  - sopratutto se è stato riconvertito da altre mansioni
- poi, per tutto il personale (*awareness*)
  - capire conseguenze in ambito cybersecurity delle normali azioni lavorative
    - social engineering, phishing, password e autenticazione
- ognuno ha un ruolo nella sicurezza aziendale

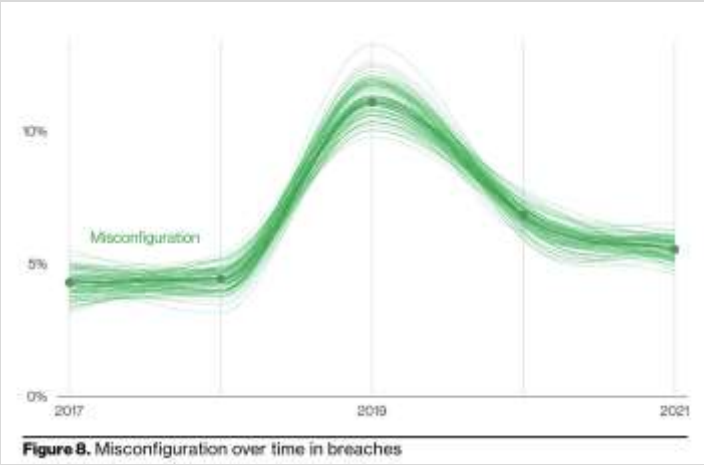


Figure 8. Misconfiguration over time in breaches

Cataldo Basile
cataldo.basile@polito.it

Prepararsi ad affrontare gli incidenti

- bisogna rassegnarsi, prima o poi verremo attaccati...
  - però possiamo influire drasticamente sulle conseguenze
- *incident response* andrebbe preparata (quasi) militarmente
  - definire cosa fare per le più frequenti tipologie di attacco
  - es. prove di evacuazione per prevenzione incendi
    - NIST SP 800-61 Rev. 2
    - ENISA good practice guide
      - https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management

Cataldo Basile
cataldo.basile@polito.it

Il Monitoring è essenziale

- per capire se si è stati attaccati
  - e che danni hanno fatto
- ma anche capire se ...
  - si è sotto attacco
    - e bloccare la propagazione
  - si è obiettivo di qualche categoria di criminali
- ridurre i tempi di reazione e individuazione

  = ridurre i danni
  - es. NIST SP 800-137

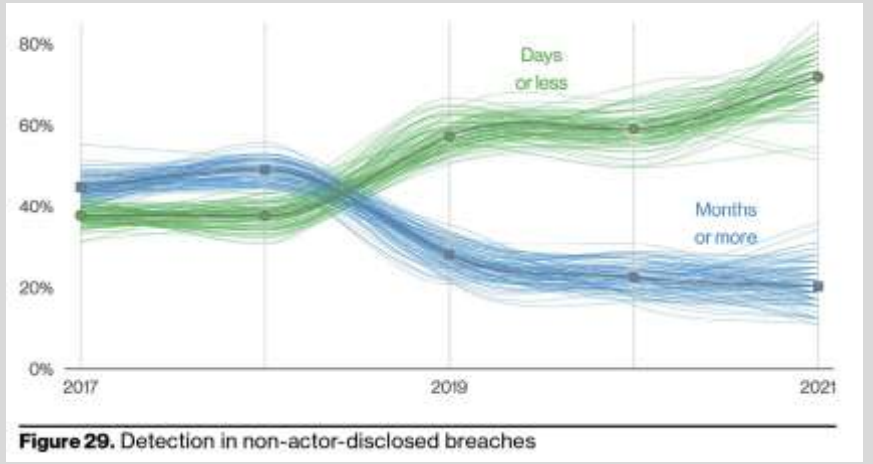


Figure 29. Detection in non-actor-disclosed breaches

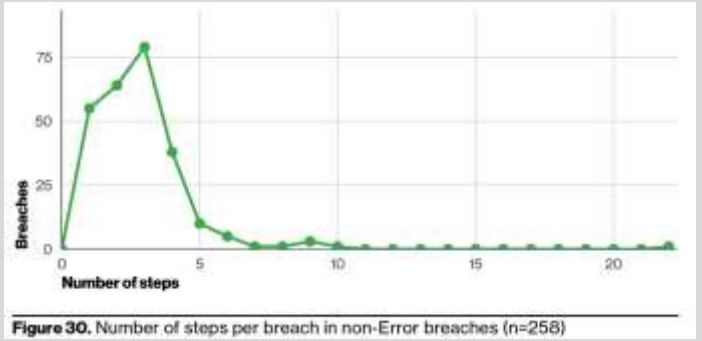


Figure 30. Number of steps per breach in non-Error breaches (n=258)

Cataldo Basile
cataldo.basile@polito.it

Domande?

Cataldo Basile
cataldo.basile@polito.it