Politiche e procedure di sicurezza: verifiche e misure

A cura di

Natale Prampolini e Pietro Brunati

Licenza CC-BY-SA 3.0

Siete liberi di… riprodurre, comunicare, condividere, modificare quest'opera (anche per fini commerciali) …ma alle seguenti condizioni… attribuzione agli autori …condivisione secondo lo stesso modo.

Le informazioni riportate in questa presentazione, ivi incluse, ma non limitate a, immagini, testo, video, foto e animazioni, ove non indicato diversamente, sono di proprietà degli autori. Le informazioni contenute in questa presentazione sono ritenute essere accurate alla data della pubblicazione. Esse sono fornite per scopi meramente didattici e non per essere utilizzate direttamente in progetti di qualsiasi tipo e servizi di consulenza. Le informazioni contenute in questa presentazione sono soggette a cambiamento senza preavviso. Gli autori non si assumono alcuna responsabilità per il contenuto di questa presentazione

Obiettivi della presentazione

Il termine **controllo** in Italia non piace, **PKI** è troppo inglese, ma se non abbiamo dei riscontri e delle verifiche come facciamo a sapere se tutte le pagine di norme e metodi di comportamento che abbiamo scritto sono utili e utilizzate.

Questa presentazione vuole dare qualche esempio, molto pragmatico e derivato dalle esperienze, di verifiche su politiche e procedure.

Valutare l'**efficacia**

Valutare l'**efficienza**

Politiche e procedure di sicurezza

La sicurezza può essere definita come la "conoscenza che l'evoluzione di un sistema non produrrà stati indesiderati". In termini più semplici è: sapere che quello che faremo non provocherà dei danni.

Quindi prescrizioni, obblighi, modalità di comportamento, di fare e non fare hanno l'obiettivo di minimizzare i rischi di eventi negativi.

- Non correre!
- Non sudare!
- Mettiti la felpa! (Solitamente lo dice la mamma quando la mamma ha freddo…)

Comportarsi minimizzando i rischi e in conformità alle norme è apparentemente noioso, faticoso, sgradevole, da evitare o eludere.

- Non parcheggiare qui, è vietato;
- Non superare i 50 km/h;
- Non passare qui, è ZTL;
- Tenere la destra…

Privacy: D.Lgs. 196/03 e s.m.i.

Punto della norma	Prescrizione: misura minima e idonea	Controllo, Misura	Risultati
Allegato B, Punti 1-15	Autenticazione e autorizzazione: caratteristiche password	Lunghezza, durata	% a norma
Allegato B, Punti 16-17	Antivirus, Firewall, Aggiornamento protezione Sistemi	Frequenza aggiornamento	% a norma
Allegato B, Punti 18, 23	Salvataggio dati e ripristino	Quali, come	Ripristino
Allegato B, Punto 20	Cifratura dati sensibili o separazione	Quali, come	PT, VA?
Provv. 1-3-07	Regolamento email e internet	Strumenti	Violazioni?
Provv.27-11-08	Amministratori di Sistema	Strumenti	Violazioni?
Provv. 3-6-11	Dati bancari	Strumenti	Violazioni?

ISO 27001 (1/2)

Punto della norma	Obiettivo di controllo	Controllo, Misura	Risultati
7.1.1	Asset Inventory	Lunghezza, durata	% a norma
7.2	Classificazione delle informazioni e etichettatura	Frequenza aggiornamento	% a norma
8	Risorse Umane	Quali, come	Gestione
10.6	Reti WiFi	Quali, come	PT, VA?
10.7	Data Loss Prevention	Strumenti	Violazioni?
10.8	Log delle operazioni	Strumenti	Violazioni?
11	Controllo accessi	Strumenti	Violazioni?

ISO 27001 (2/2)

Punto della norma	Obiettivo di controllo	Controllo, Misura	Risultati
12.6	VA / PT	Lunghezza, durata	% a norma
13	Gestione Incident	Frequenza aggiornamento	% a norma
14.1.5	Test BCP	Quali, come	PT, VA?

Norme varie

Argomento	Obiettivo di controllo	Controllo, Misura	Risultati
Analisi del rischio	Frequenza di accadimento / Probabilità dell'evento negativo	Incidenti di sicurezza	Numerosità nell'anno
	Impatto	Valore economico	Importo
231	Individuare le violazioni ai 12 articoli / commi	Organismo di vigilanza	Codice sanzionatorio
262	Sistema di Controllo Interno	Monitoraggio	Violazioni
SOX	Sezione 404	Controlli finanziari	Transazioni a norma
Manifestazioni sportive	Dispositivi Anti Infortunistici	Utilizzo	Conseguenze

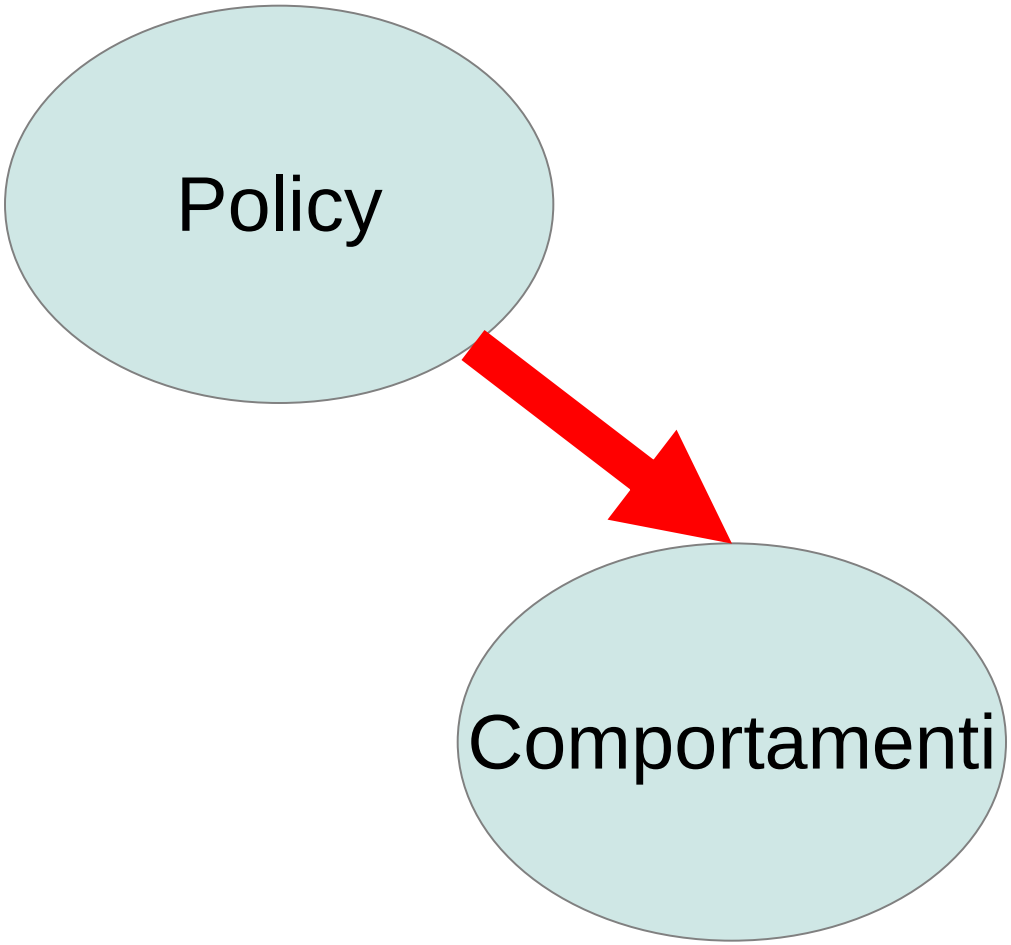
Verificare l'efficacia delle policy.

Esempio pratico: le password.

Le immagini utilizzate sono state reperite in rete e possono essere soggette a copyright dei proprietari.

Pietro Brunati

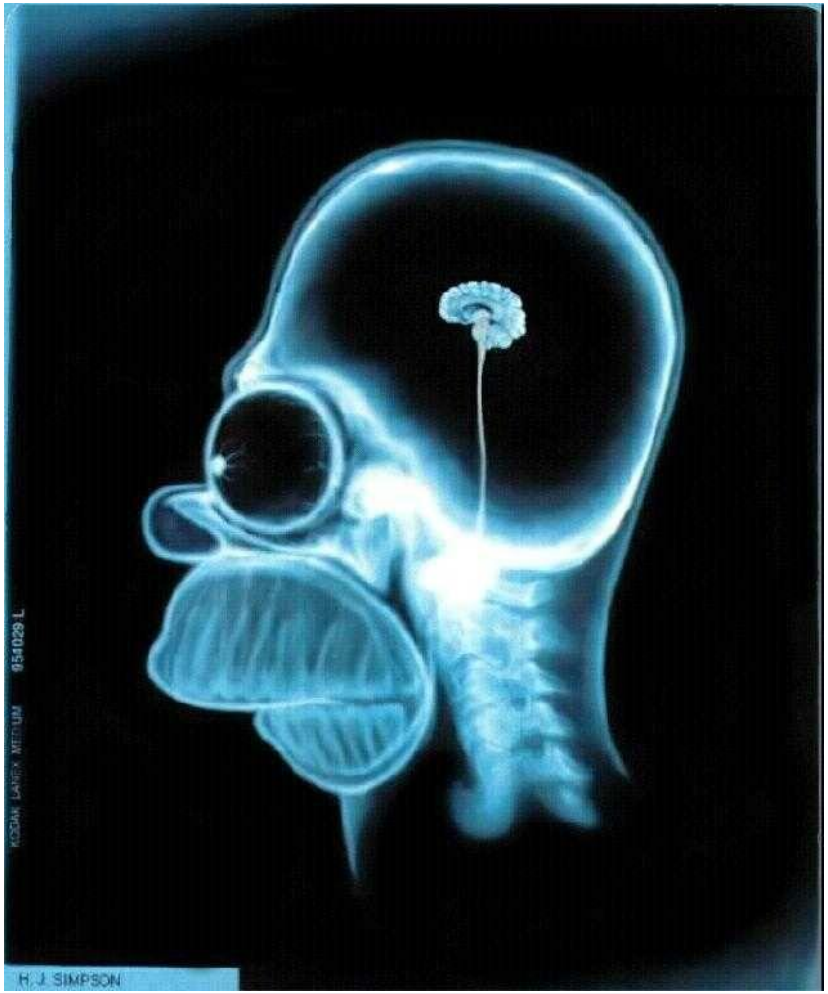
- Informatico dal 1979, saldando circuiti integrati e resistenze del suo primo computer: https://en.wikipedia.org/wiki/Nascom
- Per 30 anni Software Architect e Security Consultant.
- Manager di aziende di sicurezza informatica dal 1985.
- Ethical Hacker e Digital Forensics... dal millennio precedente.
- Fondatore ISSAF, metodologia pubblica di Penetration Testing.
- Certificato ISO-27001 dal 2006 su Security Probing: Ethical Hacking, Penetration Test, Vulnerability Assessment, Digital Forensics.

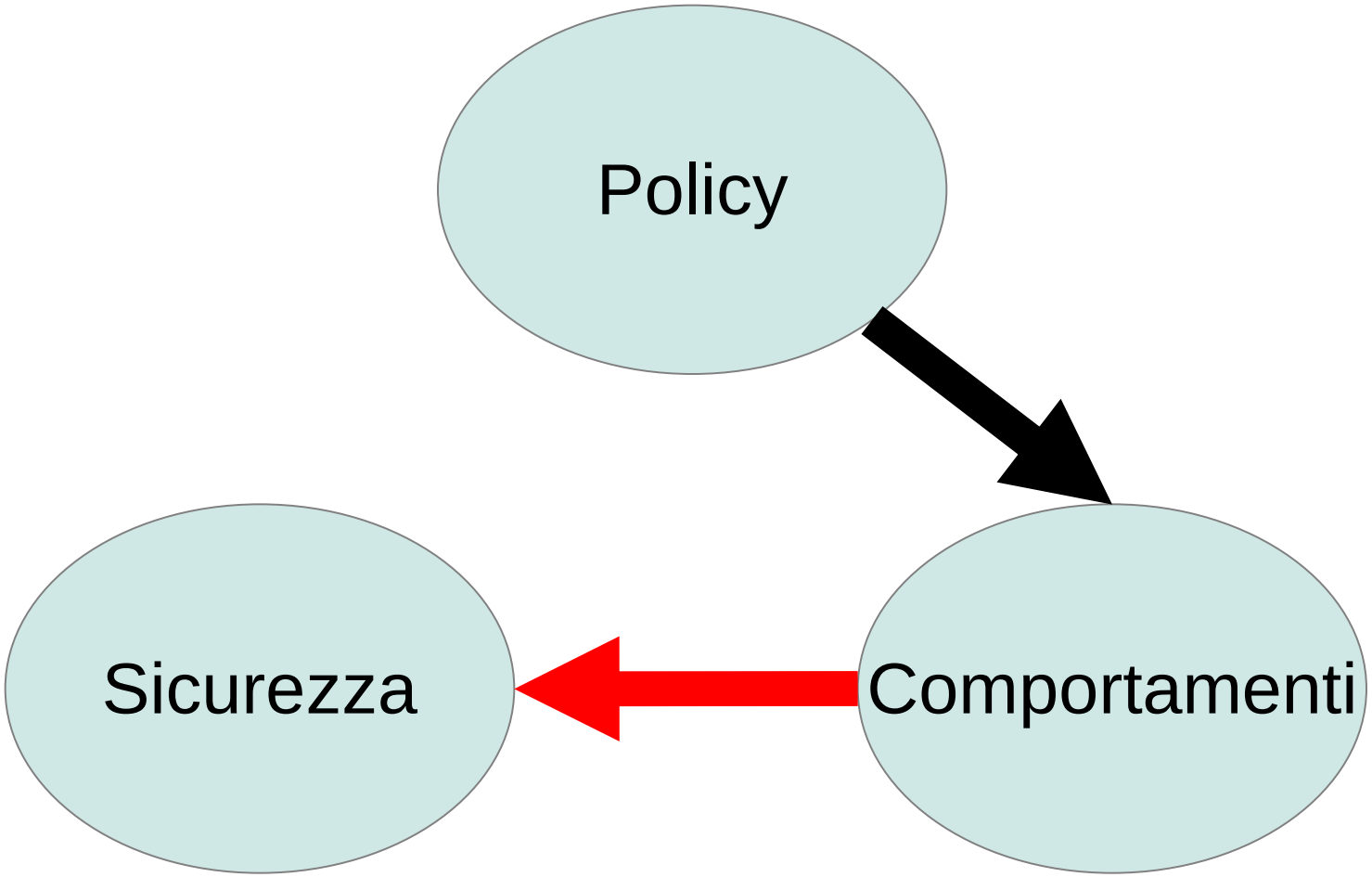

Policy
Comportamenti

Come reagisce l'utente?

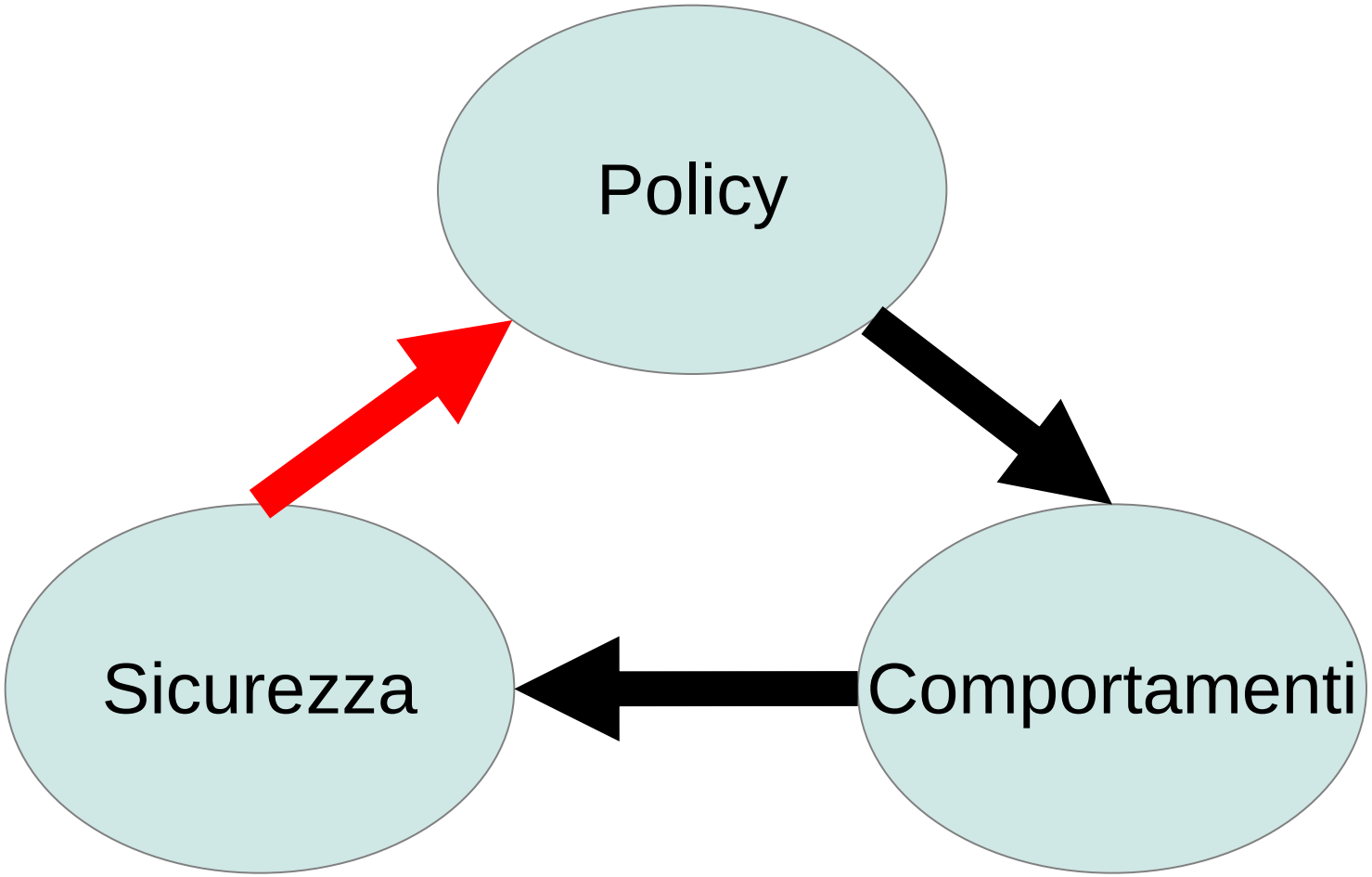
Fatica?

No, grazie.




Policy
Sicurezza
Comportamenti

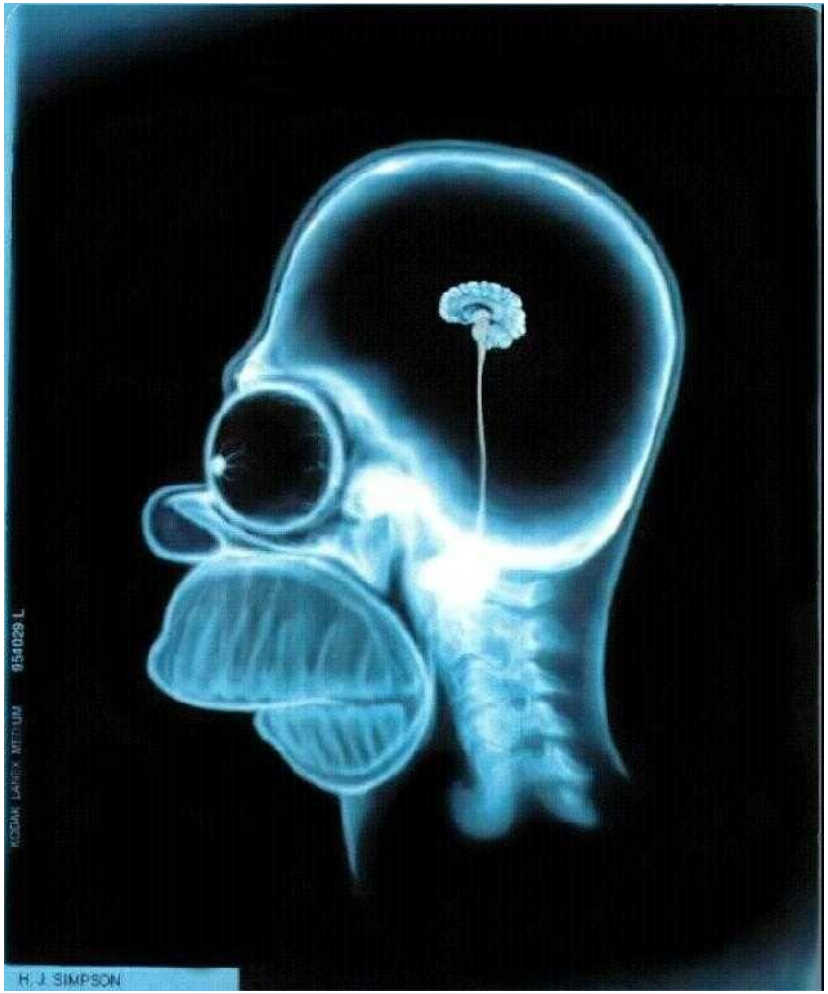
Problema #1: gli utenti.


Policy
Comportamenti
Sicurezza

Soluzione #1: policy restrittive

Uh, nuove policy!

Come posso **SEMPLIFICARMI** la vita?



Password policy più restrittive

- **Almeno 3 cifre...**
- forzaroma ==> forzaroma123
- **Almeno una maiuscola...**
- forzaroma123 ==> Forzaroma123
- **Blacklist ultime 20 password...**
- Forzaroma124 … 5 … 6 … 7 ...
- **Scadenza ogni 30 giorni...**

invece dei 90/180 prescritti dalla legge 196/03

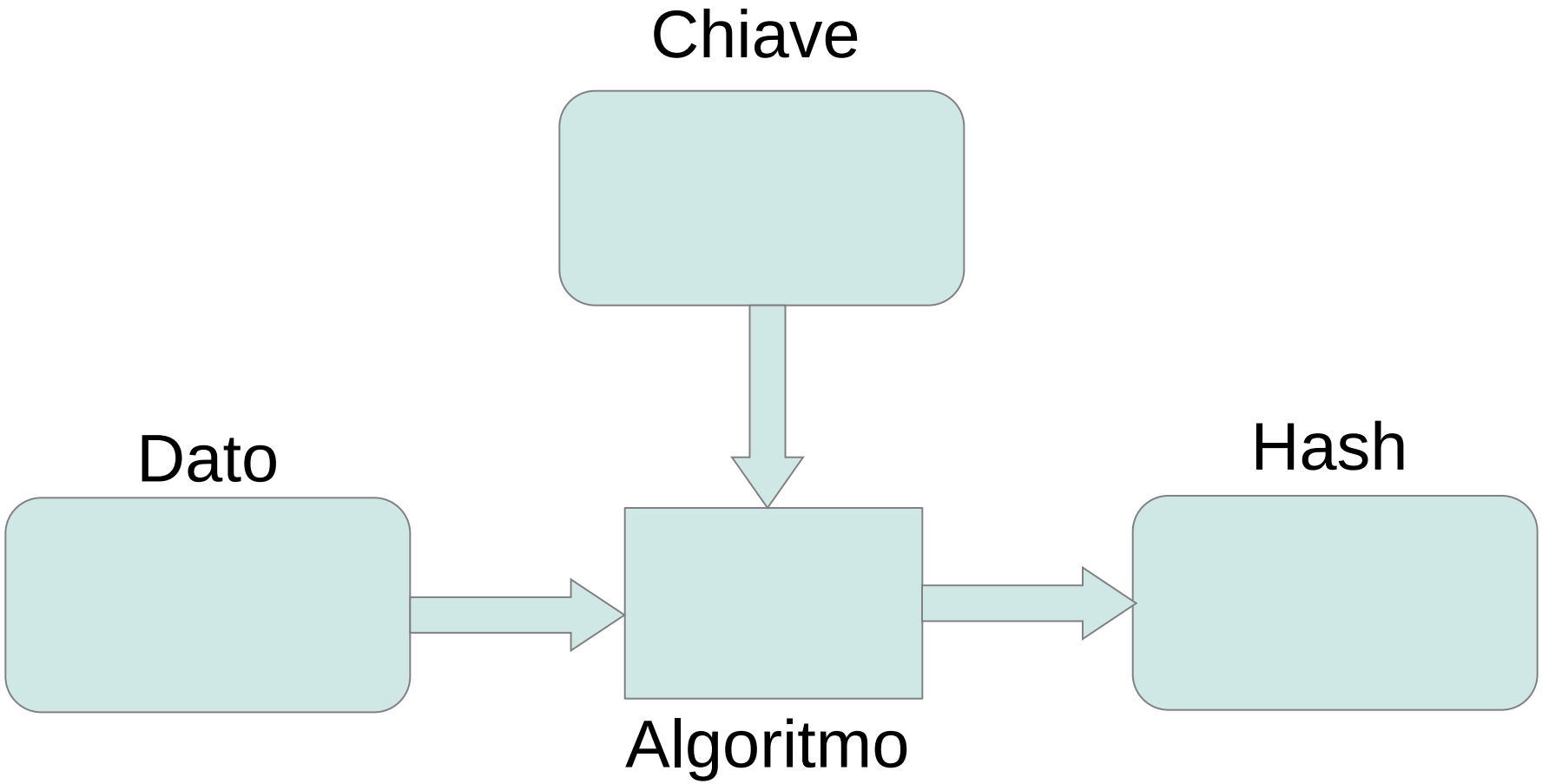
- Maggio12
- **Lunghezza minima 15 caratteri...**
- Qwertyqwerty123 *“keyboard walking”*

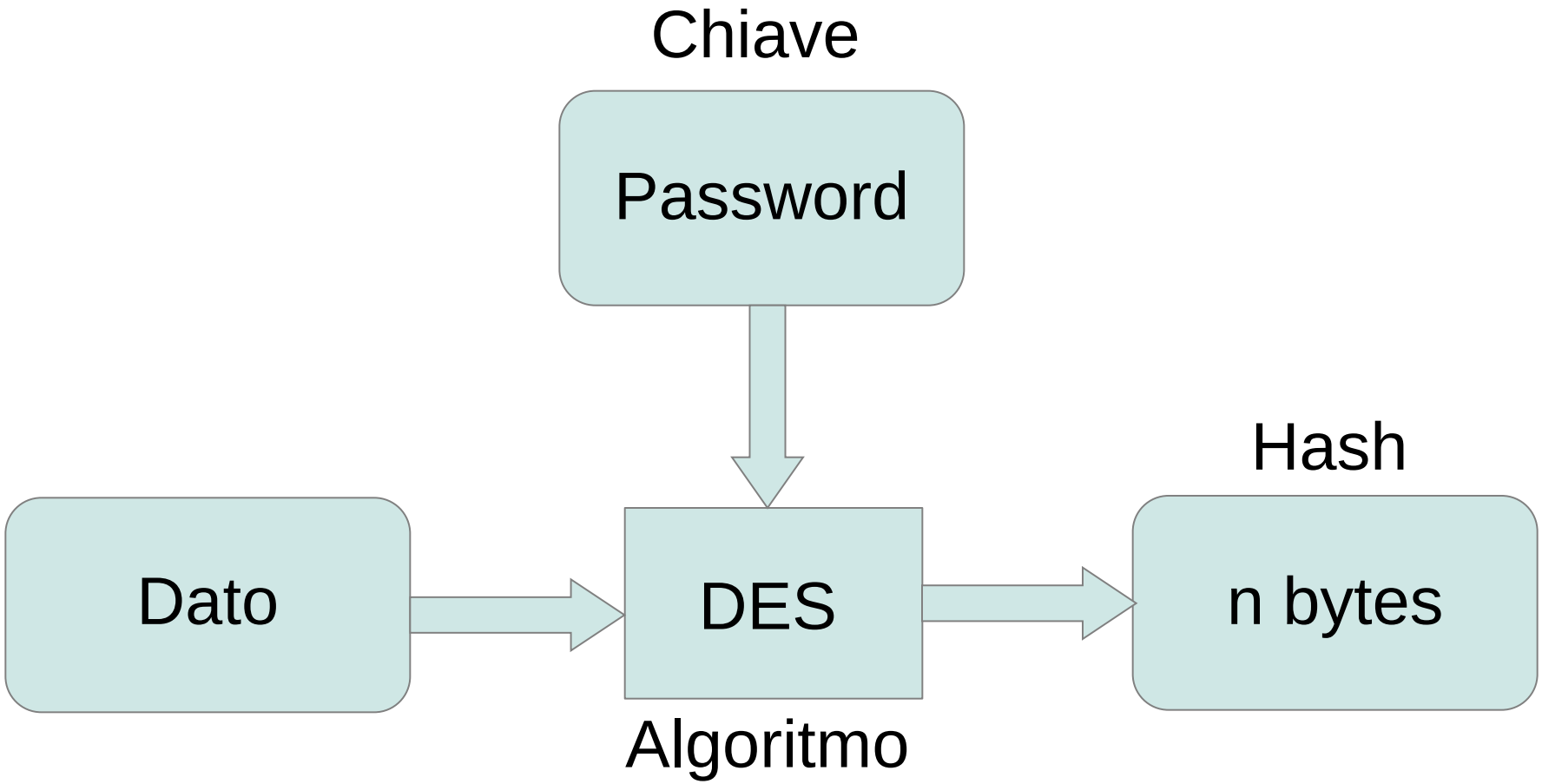
Problema #2:
Server Hashing = Password sicure?

Cosa accadrebbe se gli utenti un giorno,
per emulazione, fiducia o protesta,
si accordassero per...

**…usare una password “valida”,
ma uguale per tutti?**

Password hashing




Chiave
Password
Hash
Dato
DES
n bytes
Algoritmo

- Hashing IBM RACF DES in linguaggio “C”:

```
char dato[]= “UserID”;
des_key_schedule key1;
des_set_key (password, key1);
des_ecb_encrypt (dato, hash, key1,
DES_ENCRYPT);
```

- Differenza con Windows LM:

```
char dato[]=
   {0x4B, 0x47, 0x53, 0x21, 0x40, 0x23, 0x24,
0x25};
des_key_schedule key1;
des_set_key(password, key1);
des_ecb_encrypt (dato, hash, key1,
DES_ENCRYPT);
```

Soluzione #2?
Server Hashing = Falsa sicurezza

Meno conosciamo i sistemi,

più ci sembrano sicuri.

Problema #3: Password Sharing

www.pmi.it - “Responsabili IT trascurano Sicurezza e Privacy”

•...la gran parte del personale IT non adotta comportamenti conformi alle policies aziendali, addirittura, **compiendo attività illecite**: il 74% abusa del proprio ruolo per accedere ad informazioni riservate degli altri lavoratori, mentre il 54% viola le policy aziendali scaricando contenuti illegalmente...

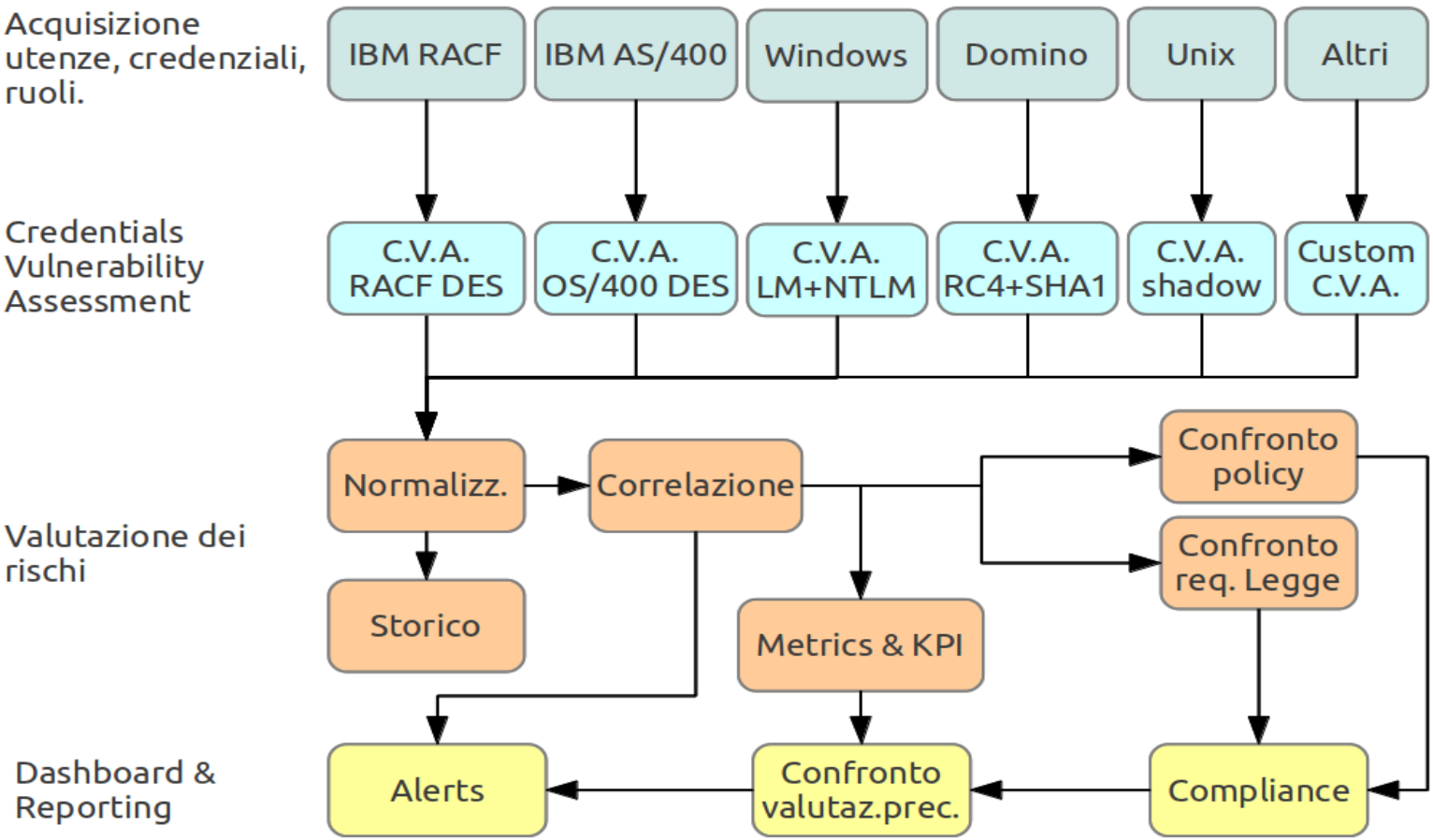
•Il pericolo vero (e la tentazione) sta nella **condivisione di password** e l’accesso condiviso con più colleghi a sistemi e applicazioni aziendali per attività di amministrazione (il che avviene nel 42% dei casi). Tutto questo **espone a seri rischi, perché in caso di incidenti diventa difficile trovare il reale responsabile...**

•In media chi ha infranto le policies IT lo ha fatto almeno due volte, tra le attività illegali più gettonate c’è il download di contenuti illegali praticato dal 54% dei responsabili IT; la creazione di regole eccezionali nei sistemi IT come firewall per ragioni personali (48%); il prelievo di informazioni aziendali (29%); la visione di file riservati relativi ai colleghi presenti nei server dell’azienda, come buste paga etc. (25%); la lettura delle email dei colleghi (16%); la cancellazione o modifica dei file di gestione dei log (15%).

Problema #4:
Cross-site passwords

Un **sistema sicuro**
è vulnerabile
se si usa una password simile
a quella di un **sistema debole**.

Sistema di monitoraggio e reporting



Sistemi analogamente vulnerabili

- Windows (tutti)
- IBM RACF
- IBM AS/400
- DB SQL (Oracle, Microsoft, MySql, …)
- SAP
- Domino
- Linux/Unix/Solaris/...
- VNC
- Cisco IOS e PIX
- Kerberos 4 e 5
- Ldap
- Varie Web Apps
- SIP VoIP
- Radius PSK
- MDx e SHAx (tutti)
- IKE-PSK VPN

Esempi di valutazioni

- Interazione sicurezza credenziali sistemi diversi
  % successo cracking del sistema(a) con mangling delle password del sistema(b)
- Interazione sicurezza utenti di sistemi diversi
  % password "simili" per stesso utente su sistemi diversi
- Verifica compliance EFFETTIVA legge 196/03
  da password cracking
- Numero password non corrispondenti a password policy
- Top passwords, top patterns, top words, top numbers, ...
- Correlazioni di utenze tramite password
- Efficacia policy (metodo grossolano)
  Percentuale di password scoperte dopo X minuti di cracking

Password risks reporting

- Legge 196/03
- Policy aziendali
- Policy utenze privilegiate (es. AdS)
- Protezione utenti apicali

Soluzione: ciclo di lavoro

1. Verificare la situazione iniziale
2. Calcolare il livello di rischio iniziale
3. **Misurare l'efficacia delle policy**
4. Migliorare le policy, più semplici ed efficaci
5. Monitorare le variazioni del rischio nel tempo
6. Suggerire/applicare le contromisure tecniche
7. Ripartire dal punto 3

Alcuni approfondimenti generici

- Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords
  by Matt Weir, http://reusablesec.blogspot.it

- Of Passwords and People: Measuring the Effect of Password-Composition Policies
  by NIST, vari autori.

Spunti di riflessione

- **Perché verificare tutti gli utenti, specialmente quelli privilegiati o apicali?**

I “difensori” devono coprire tutti i punti attaccabili, mentre agli “attaccanti” è sufficiente identificare un solo punto vulnerabile da aggredire.

- **Gli utenti sono spesso l'anello più debole della catena.** Sono protetti dalle password, ma le odiano.
- **Policy rigide o complesse causano più rifiuto, non più sicurezza.** Gli utenti sono più creativi nel trovare modi per aggirare le policy che nel pensare una buona password.
- I sistemi di autenticazione non memorizzano le password, solo hash “irreversibili”. Quindi **non possono verificare quanti utenti usano password uguali, e quindi deboli.**
- Gli hash delle password sono considerati sicuri perché sono calcolati in modo irreversibile: “1 way”. **Esistono tecniche di cracking sempre più evolute**: Markof, Rainbow, Probabilistic, GPU, Strategy-based, ecc.
- Le **dinamiche sociali** delle password non possono essere valutate senza valutare le password stesse.

Grazie per l'attenzione

pietro.brunati@br1tech.eu

prampolini@ordine.ingegneri.vi.it