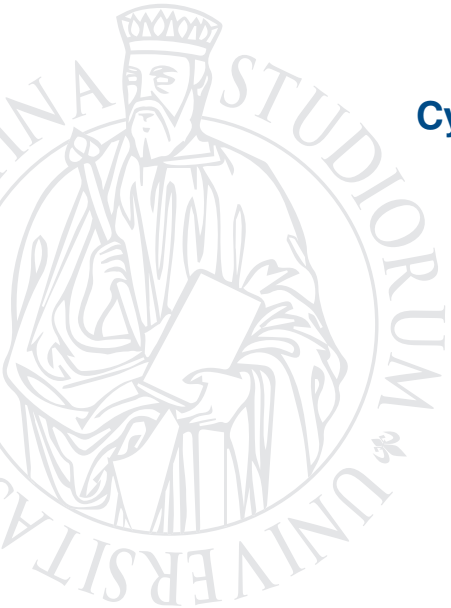

Cybersecurity e la politica dello struzzo

Sapere per difendersi

Tommaso Pecorella

tommaso.pecorella@unifi.it

Outline

Miti (da sfatare)

Un po' di dati...

Niente panico (ok, panico)

Prima di tutto gli struzzi...

Non è vero che nascondono la testa sotto la sabbia...

O almeno non lo fanno per scappare dalle responsabilità (anzi).

Quindi non abbiamo scuse.

... e dopo la CyberSecurity

Domande amletiche:

1. Si mangia? (no)
2. Mi interessa? (dovrebbe)
3. Mi tocca da vicino (purtroppo si)

`https://en.wikipedia.org/wiki/Computer_security`

> *Computer security, cybersecurity or information technology security (IT security) is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide*

`https://www.merriam-webster.com/dictionary/cybersecurity`

> *Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack*

CyberSecurity - la definizione inganna

Se ci si ferma alla definizione, la reazione (ovvia) è: **non mi riguarda direttamente**.
... ed ecco il proverbiale struzzo.

Reazioni comuni:

- Sono solo un utente, mica gestisco un server.
- Tanto ho tutto in cloud.
- Mica attaccheranno proprio me.

Sono tutti e tre argomenti invalidi:

- Non è vero, gestisci moltissimi dati: i tuoi.
- Il cloud è solo una delega di responsabilità. Devi delegare bene.
- No, attaccheranno proprio te, perché non ti sei protetto.

Dati, ci piacciono i dati obbiettivi

Quanto costa la CyberSecurity (o la sua mancanza)?

Difficile dirlo, ma possiamo guardare quanto vengono pagati i bug...

- Google: da $100 a $31,337
  `https://www.google.com/about/appsecurity/reward-program/`
- Apple: da $100,000 a $1,000,000
  `https://developer.apple.com/security-bounty/`
- Android: da $100,000 a $1,000,000
  `https://www.google.com/about/appsecurity/android-rewards/index.html`

Lista pubblica: `https://hackerone.com/bug-bounty-programs`

Nota: trovare un bug "ben pagato" è più difficile di quanto uno non pensi.
Nota (2): è una questione di mercato...

Pericoli e conseguenze...

Esempi recenti:

Solarwinds

- Circa 18.000 "targets", tra cui entità del governo federale USA.
- Pare che il tutto sia originato da una password (solarwind123).

gab leaks

- Circa 70 gigabytes di dati trafugati.
- Il CTO aveva rimosso i controlli dal codice.

parler scraping

- Praticamente tutte le conversazioni, immagini, etc..
- 'Absurdly Basic Bug'.

Pericoli e conseguenze (2)...

Logix PLCs

- Severity score 10/10.
- Viva l'industria 4.0.

supply chain attacks

- A rischio (quasi) tutti i moderni sistemi di programmazione.

Impianto idrico di Oldsmar (Florida)

- Tentativo di inquinamento acqua potabile - circa 15.000 utenti.
- Controllo remoto senza VPN e con password unica per tutti i controllori.

E questi sono solo alcuni scoperti nell'ultimo mese !

Dobbiamo preoccuparci?

... no, dobbiamo *occuparci* [della sicurezza].

Cosa serve:

- Metodo scientifico
  trovare le vulnerabilità è ancora un'arte, dobbiamo farla diventare una scienza.
- Approccio "by design"
  la sicurezza dovrebbe essere un requirement, non qualcosa che si fa "dopo".
- Cambio culturale
  gli utenti devono *pretendere* la sicurezza dei prodotti che usano (e saperla valutare).

Esempio: comprereste una macchina senza airbag?

... e lo struzzo?

Lo struzzo (non quello vero) preferisce non sapere. Non è più possibile fare gli struzzi.
ci sarebbero anche le tre scimmiette...

La mancanza di sicurezza porta a:

- Aziende: perdita di IPR, spionaggio industriale, blocco della produzione, etc.
- Privati: perdita di privacy, furto di identità, blocco di sistemi "smart", etc.

Certo, è più facile "pensarci dopo", ma è anche molto più costoso e difficile.

Back to the original question: mi riguarda?

Spoiler alert: si, no, forse.

Il primo elemento indispensabile è *culturale*.

- L'importanza dei dati in un mondo digitale (la loro proprietà, chi ci fa cosa).
  esempi: TikTok, Amazon, Facebook, Google, etc.
- Il concetto stesso di sicurezza di un sistema.
  esempio: cosa fanno *davvero* le applicazioni che usiamo.
- Quali diritti hanno gli utenti.
  Quanti di voi hanno letto un'EULA, o sono andati a leggere il trattamento dei dati.
- Il concetto di identità digitale.
  ... e come proteggerla - "maga2020!" non è una buona password.

Back to the original question: mi riguarda?

Il secondo elemento è *la capacità di valutazione*.

Esempio pratico: compro una macchina senza l'ESP - good? bad?

Nella sicurezza si parla di asset *primari* e *secondari*:

asset primario

Se viene compromesso si blocca tutto (o quasi).
Vanno protetti ad ogni costo.

asset secondario

Se viene compromesso non piango (troppo).
Devono essere presenti delle *contromisure*.

Dovremmo usare sempre metri di giudizio informati.

Back to the original question: mi riguarda?

Il terzo elemento è *tecnico*.

Certificazioni

Serve un sistema di certificazione della sicurezza dei prodotti/sistemi.
Per ora ci dobbiamo fidare del produttore. Non è una buona idea.

Sistemi di sviluppo e verifica

Qui si tocca un nervo scoperto.
La sicurezza significa fare le cose per bene (e questo costa).

Dare importanza alla sicurezza dei sistemi

I sistemi devono essere progettati per essere sicuri.
E' molto più complicato di quanto uno non pensi.

Compiti per casa...

Domande da porsi...

1. La mia identità digitale è al sicuro? (password, programmi in uso).
2. Il mio sistema è al sicuro? (firewalls, connessioni protette).
3. I miei asset sono sicuri? (aggiornamenti, supporto).
4. Mi tengo informato? (leggere molto).

Suggerimento: `https://www.arstechnica.com`