SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Ospedaliero - Universitaria di Parma

Sviluppare la coscienza informatica attraverso attacchi etici

Incrementare il livello di "coscienza" sugli aspetti di sicurezza informatica riguardanti la tutela delle credenziali personali, attraverso attacchi di tipo etico e opportunità di formazione

Sviluppare la coscienza informatica attraverso attacchi etici

- Dai primi DoS: *Ping of death……*

- *Firewall, IPS, AV, NGAV, AS, WAF, NAC, SIEM, EPP+ EDR, deception, ……*
- *Analisi Comportamento, Machine Learning*

Sviluppare la coscienza informatica attraverso attacchi etici

- …… non si riesce a spedire posta a…..
  - Ore di indagini…..
    - ……inseriti in RBL ……quando va bene….
- *Ore di form compilate nei giorni successivi per uscire dalle varie RBL*
- *Danno d'immagine poi……*
  - *Data Breach, denuncia agli organi competenti…..*

Sviluppare la coscienza informatica attraverso attacchi etici

---

Approccio Olistico

Vs

Approccio tecnologico

Una catena è forte quanto il suo anello più debole…… qual è?

Sviluppare la coscienza informatica attraverso attacchi etici

---

L'impianto tecnologico dedicato alla sicurezza è governabile attraverso tempo uomo non dedicato?

…… abbiamo unità operative dedicate alla sicurezza?

Occorre equilibrare i due approcci secondo normativa e risorse…..

Sviluppare la coscienza informatica attraverso attacchi etici

Altri servizi si stanno affacciando da diversi anni al mondo ICT (PLC, UTA, MD, eccetera) senza avere coscienza della sicurezza informatica

Sviluppare la coscienza informatica attraverso attacchi etici

… opportunità di Tirocinio

Focalizzazione sul trattamento dati:

- Analisi d’ impatto
- Informativa
- Corrispondenza normativa

Sviluppare la coscienza informatica attraverso attacchi etici

Progetto controllo degli accessi

- Aumento consapevolezza degli utenti sull'utilizzo delle proprie credenziali
- Verifica degli accessi anomali (fuori orario servizio, elevato numero login falliti, ecc.)

Progetto simulazione attacco Etico

- Progetto di Tesi
- Personalizzato e multicanale Phishing e altro

Ulteriori Sviluppi …

- Social Engineering Attacks:
  - Bad USB Hacking
  - Pretexting
  - Base

Sviluppare la coscienza informatica attraverso attacchi etici

Sviluppo di un sistema di Identity Management

Per tutti gli utenti (interni, consulenti etc.)

- Reset password utente autonomo con quesito segreto
- Richiesta abilitazioni utente tramite modulo online con profili abilitativi strutturati:
  - Responsabile trattamento
  - Responsabile della richiesta
  - Gestore del ciclo di vita della richiesta

Sviluppare la coscienza informatica attraverso attacchi etici

Sviluppo di un sistema di Identity Management

Per gli utenti amministratori (interni/esterni):

- Doppia utenza amministrativa (come previsto dalle misure minime AGID)
- Nessuna utenza «di gruppo» o «applicativa» ➔ solo utenze riconducibili a persone fisiche

Sviluppare la coscienza informatica attraverso attacchi etici

Verifica degli accessi utente

- Indiretta
  - fuori orario servizio amministratori
  - elevato numero login falliti
  - Numero di login sui DB / Server
- Diretta (in rilascio)
  - Portale verifica autonoma login
  - Segnalazione login su nuovi devices

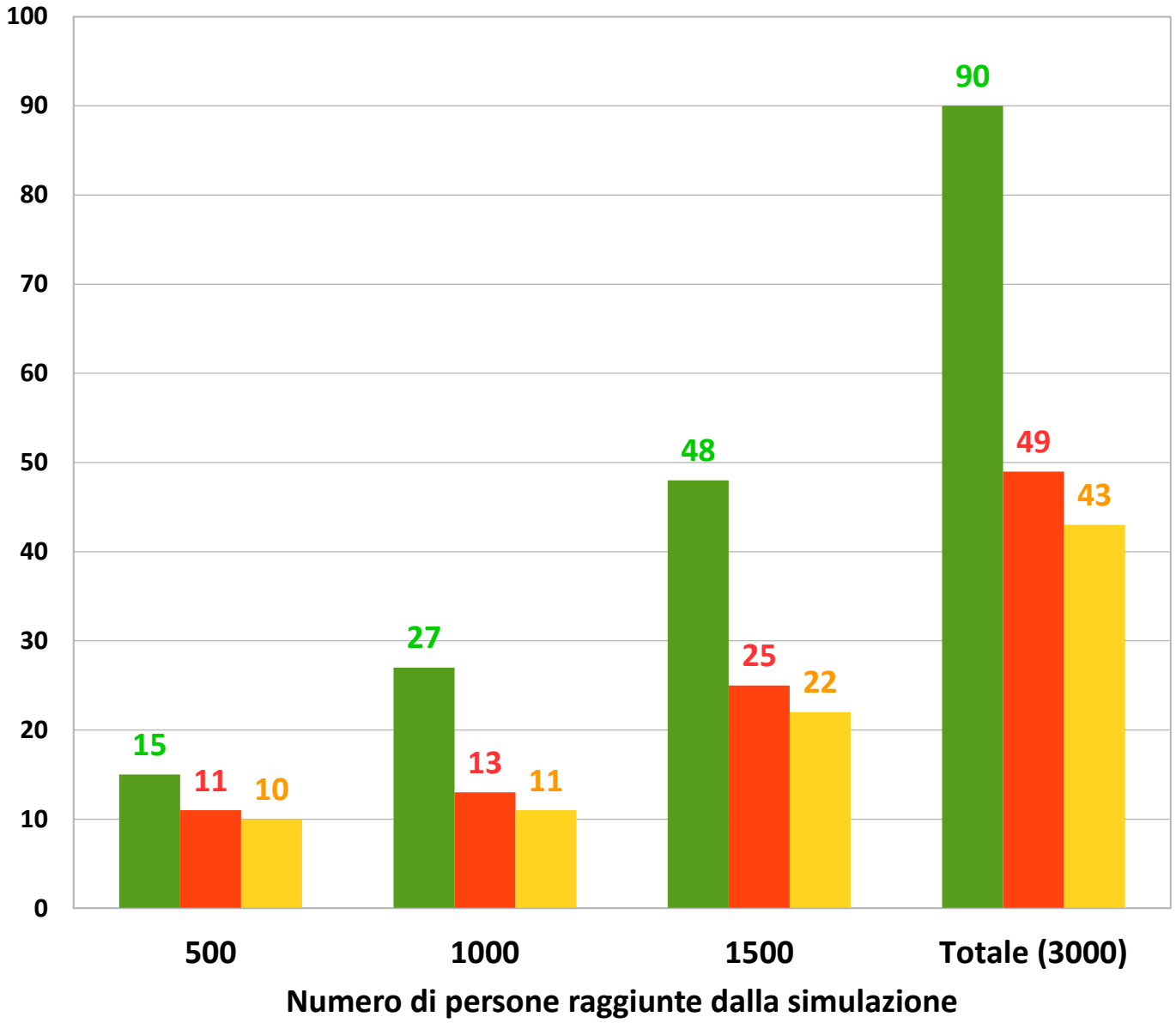
Progetto Phishing: Perchè

- **INFRASTRUTTURA INTERNA**
  - Pieno controllo sull'uso (dalla scrittura alle grant sull'utilizzo) in accordo con DPO e Gruppo Privacy
  - Customizzabilità verticale sulla realtà
  - Pieno controllo sui dati utilizzati/memorizzati
  - Possibilità estensione del progetto step-by-step
- **INTERFACCIA SEMPLICE**
  - Non è necessario conoscere l'infrastruttura ospedaliera

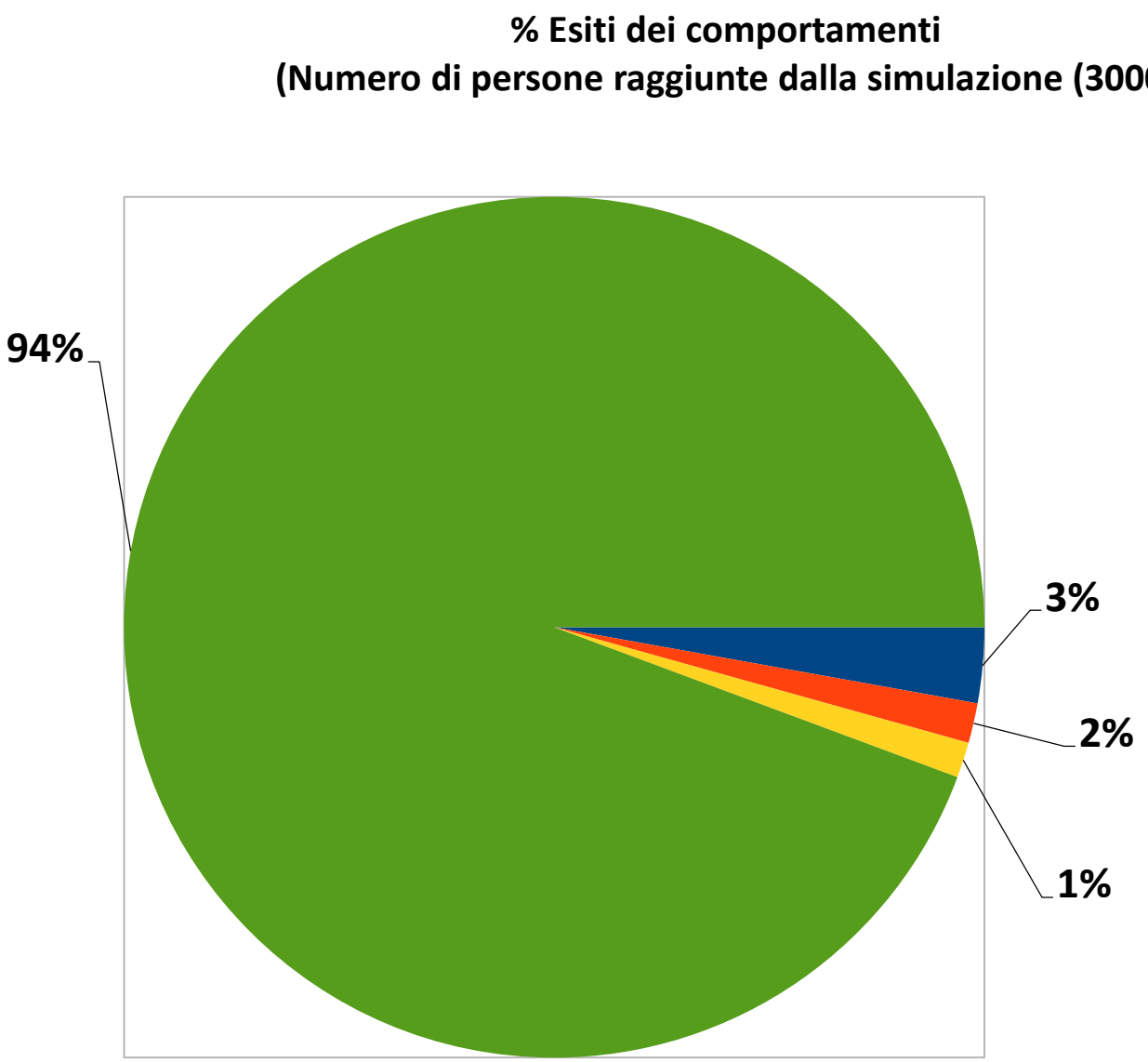
Progetto Phishing: L'implementazione

1. **PLANNING**:
   - ***deceptive phishing:*** Mail fraudolenta verso sito fake interno «cammuffato» ➔ viene richiesto l'inserimento credenziali aziendali
2. **SETUP**:
   - Query LDAP
3. **ATTACK**:
   - Invio massivo (1:1 utente/mail)
4. **COLLECTION**:
   - Registrazione dei singoli invii su DB
5. **DATA ANALISYS**:
   - Analisi dei comportamenti ricevuti dal sito fake
6. **PROPOSTA FORMATIVA**

Progetto Phishing: Data Analisys



Progetto Phishing: Data Analisys



Progetto Phishing: L’evoluzione

- **CORSO CON U.O. FORMAZIONE**
  - Pagina informativa per l’utente finale con proposta di corso e-learning
  - Corso proposto: accreditato ECM su piattaforma AVEN
  - Previsto test finale di verifica con attestato digitale

- **FEEDBACK E RI-SOTTOMISSIONE**
  - Possibilità di registrare gli accessi e il superamento del test
  - Sottomissione di un nuovo attacco alle vittime per feedback

Sviluppare la coscienza informatica attraverso attacchi etici

---

GRAZIE PER L'ATTENZIONE