FPA

DIGITAL 360

FATTORE UMANO E SICUREZZA DELL'END POINT

Ing E. Veiluva – DPO
CSI Piemonte

Perché un documento su Fattore Umano e la difesa dell'end point

Il 46 % degli attacchi informatici avviene sfruttando le debolezze del fattore umano.

Fonte: The Human Factor in IT Security (Kaspersky Lab)

Temi Affrontati

1. *La sensibilizzazione come fattore abilitante alla consapevolezza del rischio Cyber.*
2. *La determinazione delle linee guida "organizzative e "comportamentali" : canalizzare il modus operandi*
3. *La condivisione delle competenze: - la figura del focal point*
4. *Il percorso per educazione Cyber: la formazione dal livello decisionale all'operativo - suggerimenti pratici*
5. *I punti cardine da presidiare nella difesa dell'end point*

La sensibilizzazione come fattore abilitante alla consapevolezza del rischio Cyber

«Spesso non ci si chiede cosa vi sia dietro un click o cosa comporta accettare l'utilizzo di un'app o verificare come opera l'app installata nel loro dispositivo.

Spesso non si riesce neanche a leggere con attenzione una e-mail»

La determinazione delle linee guida «organizzative» e «comportamentali»

«La definizione e formalizzazione di regole comportamentali chiare e, possibilmente, semplici da applicare per gli utilizzatori.
Nell'impianto documentale base dell'organizzazione deve prevedersi una metodologia per la Categorizzazione delle informazioni in modo da contenere, entro limiti accettabili, il rischio di compromissioni della riservatezza, integrità e disponibilità delle stesse.»

La condivisione delle competenze: la figura del focal point

«Favorire l'istituzione di figure di focal point che operino all'interno degli uffici degli Enti.
Il ruolo di queste figure è fondamentale:
supportare, aiutare, diffondere tra i colleghi di ufficio
la corretta sensibilità e attenzione sugli aspetti
di sicurezza nell'operatività del quotidiano»

Il percorso per l'educazione Cyber: la formazione dal livello decisionale all'operativo

«Competenza e cultura si costruiscono attraverso un percorso di educazione: diventa così fondamentale la formazione a tutti gli utenti della struttura organizzativa…. Se siamo tutti più formati e consapevoli possiamo affrontare con maggiore probabilità di successo le sfide e le minacce che diventano sempre più complesse e sofisticate.»

Punti cardine nella difesa dell'end point

6.1 Autenticazione
6.2 Protezione della mail
6.3 Protezione della navigazione
6.4 La cifratura delle informazioni
6.5 Accesso ai dati
6.6 Il monitoraggio delle rete
6.7 Il controllo dispositivi mobili
6.8 L'attenzione ai social

IL DECALOGO parte 1

1	Definire l'organizzazione e le regole per la sicurezza: Responsabile e controlli	Hai definito il perimetro di azione? Puoi migliorarlo
2	Definire il perimetro di azione? Si può migliorare?	Hai valutato i Rischi? Sono cambianti?
3	Valutare i Rischi e definire una soglia di accettabilità?	Hai misura il posizionamento definendo una soglia di accettabilità
4	Fornire istruzioni chiare e condivise ai dipendenti: regolamenti interni, circolari, disposizioni: aggiornare la documentazione	Hai definito una strategia di sicurezza? Puoi farla evolvere?
5	Attuare le adeguate contromisure organizzative, tecniche e tecnologiche: le Misure Minime di Sicurezza (MMS) di AgID e GDPR	Hai verificato l'applicazione dei processi base (update del sistema operativo, backup, etc)?

FPA
DIGITAL360

IL DECALOGO parte 2

6	Sensibilizzare a tutti i livelli sugli aspetti di sicurezza delle informazioni	Hai sensibilizzato ed erogato la formazione a tutti i livelli? E' aggiornata?
7	Effettuare formazione e addestramento del personale sui principali aspetti di sicurezza	Hai misurato la comprensione e la penetrazione di quanto applicato al punto precedente?
8	Proteggere i servizi base (mail, navigazione, sistemi, autenticazione) dell'ente.	Hai protetto i tuoi servizi base (mail, navigazione, sistemi, autenticazione, interscambio)? L'hai verificato?
9	Verificare periodicamente l'efficacia dei controlli attuati: test di addestramento del personale, verifica vulnerabilità, ecc…	Hai fornito istruzioni chiare ai dipendenti? Sono aggiornate?
10	Misurare	Hai misurato i risultati ottenuti dai punti precedenti?
		Se la risposta è si RIPARTIRE da 1 ☺

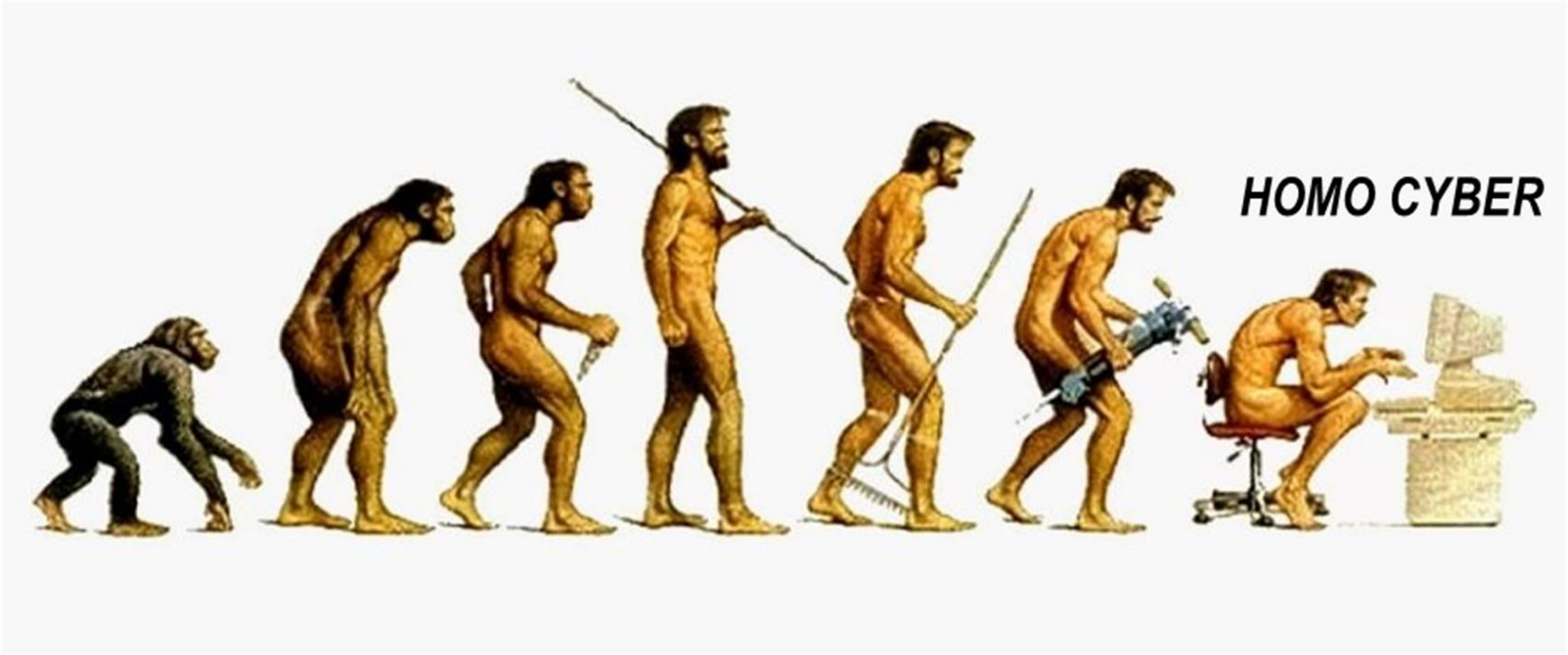
Conclusioni

«La tecnologia deve quindi essere in grado di monitorare, acquisire ed adattarsi ai bisogni reali dell'individuo, affinché diventi sempre più mitigabile l'errore introdotto dal "fattore umano". Diventa fondamentale in ogni PA la formazione, dove la sensibilizzazione al rischio Cyber coinvolga tutto il personale non solo gli specialisti del settore IT ma innanzitutto la componente manageriale.»

Ringraziamenti

Un ringraziamento doveroso a FPA ed ai partner commerciali per l'organizzazione dei lavori e in particolare a tutti i colleghi del tavolo di lavoro che hanno partecipato attivamente in prima persona alla discussione e redazione del documento , mettendo a disposizione il loro tempo e la loro esperienza per il raggiungimento dell'obbiettivo.

Grazie per l'attenzione



enzo.veiluva@csi.it

FPA
DIGITAL 360

FPA

DIGITAL 360

+39 06.68 42 51 info@forumpa.it @forumpa